تصویر ابو عبد الرحمن الکردی

گروه آموزش مهارت

رایانه کار درجه ۲

استاندارد بین المللی ۳-۴۲/۲۸

مطابق با استاندارد جدید

ویروس های کامپیوتری



مؤلفین: مهندس مجید سبزعلی گل - مهندس سید علی موسوی - مهندس مهدی قربانی



رایانه کار درجهٔ دو

مهارت هشتم

ویروسهای کامپیوتری



مـــولفیـــن

مهندس مجید سبزعلی‌گل

مهندس سید علی موسوی

مهندس مهدی قربانی

موسوی، علی
رایانه کار درجه دو: مهارت هشتم ویروس‌های کامپیوتری / مؤلفین علی موسوی، مجید سبز علی گل، مهدی قربانی. ــ تهران: صفار: اشراقی، ۱۳۸۳.
۸۰ ص.:مصور.
ISBN 964-388-070-2
فهرستنویسی بر اساس اطلاعات فیپا.
عنوان دیگر: رایانه کار درجه ۲: ویروس‌های کامپیوتری (مهارت هشتم).
۱. ویروس‌های کامپیوتر -- دستنامه‌ها. الف. سبز علی گل، مجید، ۱۳۵۲ - . ب. قربانی، مهدی، ۱۳۴۹ - . ج. عنوان. د. عنوان: رایانه کار درجه ۲: ویروس‌های کامپیوتری (مهارت هشتم).
۸۵م۹و/۷۶/QA۷۶ ۰۰۵/۸۴
کتابخانه ملی ایران ۲۶۵۴۷-۸۳م

فهرستنویسی پیش از انتشار: انتشارات صفّار

شناسنامه کتاب

نام کتاب	:	رایانه کار درجه ۲ ویروس‌های کامپیوتری (مهارت هشتم)
تألیف	:	سید علی موسوی - مجید سبزعلی گُل - مهدی قربانی
طرح جلد	:	فرهاد کمالی
لیتوگرافی	:	پویش
چاپ متن	:	چاپخانهٔ گنج شایگان
چاپ جلد	:	چاپخانهٔ ظفر
نوبت چاپ	:	اول - ۱۳۸۳
شمارگان	:	۳۳۰۰ نسخه
ناشر	:	انتشارات صفّار ـ اشراقی
قیمت	:	۹۰۰۰ ریال
مرکز پخش	:	پخش کتاب بینش ✆ ۶۴۰۸۴۸۷

شابک ۲-۰۷۰-۳۸۸-۹۶۴
ISBN 964-388-070-2

www.nasherin.com/saffar
saffar@nasherin.com

تعریف :

رایانه کار درجهٔ دو : کسی است که از عهدهٔ توانایی شناخت مبانی و مفاهیم کامپیوتر ، کار با سیستم عامل **Windows XP** ، کار با **Word** ، کار با **Excel** ، کار با **Access** ، کار با **PowerPoint** و کار با اینترنت برآید.

رایانه کار درجهٔ ۲		
کد شناسایی		۷-۱۱۰۱۰۳۳۰۱
شماره درس		۸۹۹۴ - ۸۹۹۵
کد استاندارد بین المللی		۳-۴۲/۲۸
سال تدوین استاندارد		۱۳۸۲
تعداد واحد	نظری	۵،۵
	عملی	۶،۵
	کل	۱۲
مدت دوره	نظری	۱۶۰ ساعت
	عملی	۲۹۰ ساعت
	کل	۴۵۰ ساعت
نمرهٔ قبولی (از ۲۰)	نظری	۱۰
	عملی	۱۴

رایانه کار درجه دو

مهارت اول	مبانی کامپیوتر
مهارت دوم	سیستم عامل Dos
مهارت سوم	ویندوز XP (۱)
مهارت چهارم	MS Word XP
مهارت پنجم	MS Excel XP
مهارت ششم	MS Access XP
مهارت هفتم	MS PowerPoint XP
مهارت هشتم	ویروس‌های کامپیوتری
مهارت نهم	اینترنت
مهارت دهم	Outlook Express 6

فهرست مطالب

مقدمه

پیشرفت سریع تکنولوژی، بویژه فنآوری اطلاعات و ارتباطات (ICT) ، روز بـه روز چشـم انـدازهـا و افق‌های روشن‌تری را جهت تسخیر قُلل علمی ، فنی و صـنعتی و حـل مشـکلات و مسـائلِ بشـر ارائـه می‌کند و تک‌تک افراد جامعه را به تلاش مضاعف در کسبِ مهارتهای رایانـه‌ای و کـاربرد آنهـا در سـایر علوم مُلزم می‌سازد ، بنحوی که امروزه افراد و جوامع ناتوان در بکارگیری فن‌آوریهای جدید رایانـه‌ای را بی‌سواد تلقی می‌کنند، گواه این امر پذیرش و اجرای دوره‌های مهـارت رایانـه‌کـار و سـایر مهـارت‌هـای مرتبط فنآوری اطلاعات از سوی وزارت آموزش و پرورش است.

خوشبختانه سازمان آموزش فنی و حرفه‌ای کشور نیز که متولی آموزش‌های فنی و حرفـه‌ای و تـدوین اسـتانداردهای مربوطـه در کشـور اسـت همـه سـاله و همگـام بـا پیشـرفت فـن‌آوری و نیـاز جامعـه ، استانداردهای لازم را بازنگری و اصلاح می‌نماید به همین منظور نگارش دوم استانداردهای رایانه‌کـار بـا رویکرد توانایی بکارگیری **Windows XP** و **Office XP** اصلاح گردیده است.

استاندارد آموزشی رایانه‌کار درجهٔ دو در قالب مهارت‌های زیر ارائه شده است :

رایانه‌کار درجهٔ دو				
مهارت	عنوان مهارت	زمان آموزش (ساعت)		
		نظری	عملی	کل
اول	مبانی کامپیوتر	۸/۵	۱۲	۲۰/۵
دوم	سیستم عامل Dos	۷	۱۰	۱۷
سوم	ویندوز XP (۱)	۴۰/۵	۷۳/۵	۱۱۴
چهارم	MS Word XP	۲۱	۴۸	۶۹
پنجم	MS Excel XP	۲۱	۳۷	۵۸
ششم	MS Access XP	۲۲	۵۳	۷۵
هفتم	MS PowerPoint XP	۲۰	۳۲	۵۲
هشتم	ویروس‌های کامپیوتری	۶	۱۲	۱۸
نهم	اینترنت	۷	۵	۱۲
دهم	Outlook Express 6	۷	۷/۵	۱۴/۵
جمع کل (ساعت)		۱۶۰	۲۹۰	۴۵۰

در راستای تدوین کتب آموزشی خودآموز ، مولفینِ **گروه آموزش مهارت (گـام)** بر اساس سالها تجربهٔ تدریس ، تحقیق و برنامه‌ریزی در علوم مختلف رایانه‌ای و با عنایت به نیاز مُبرم کارآموزان ، دانش آموزان و سایر علاقه‌مندان به فراگیری آموزش‌های فنی و حرفه‌ای ، اقدام به تهیه و تدوین این مجموعه بر اساس جدیدترین سرفصلِ ***استانداردهای مهارت فنی و حرفه‌ای*** **و مطابق با آخرین تغییرات کتاب‌های درسی کار دانش** با ویژگی‌های منحصر به فرد زیر نموده‌اند :

- شیوهٔ آموزشی این سری از کتابها خودآموز و گام به گام می باشد ، به همین منظور و جهت رعایت پیوستگی مطالب و سهولت در یادگیری ، در مواردی سرفصل‌های استاندارد جابجا شده است .
- تعاریف اصطلاحات و مفاهیم کلیدی به صورت پر رنگ و با رنگ متمایز مشخص شده‌اند.
- چکیده‌ای از رئوس مطالب و موضوعات ارائه شده در هر فصل ، در ابتدای همان فصل آورده شده است همچنین قبل از تشریح اغلب موضوعات ، جهت فراگیری آسان نوآموزان ، دسته بندی مناسبی از تیتر مطالب آن موضوع ارائه شده است .
- هر گام عملی با علامت ☑ در ابتدای آن مشخص شده است و حتی‌المقدور تصاویر لازم برای هر گام آورده شده است.
- بر روی تصاویر عملکرد گزینه‌ها و دکمه‌ها به همراه سایر توضیحات لازم مشخص شده است.
- نکات اساسی و تکمیلی در کادرهای مخصوص نکته ، آورده شده است.
- دکمه‌ها ، نمادها و آیکن‌های لازم برای تشریح هر موضوع ، در جای خود و در داخل متن آورده شده است ، ضمن اینکه عملکرد آنها به صورت جداگانه در جدول‌ها ویژه یا بر روی تصویر مشخص شده است.
- در انتهای هر فصل مجموعه‌ای از سئوالات تشریحی ، تستی و دستور کار آزمایشگاه برای تکمیل مهارت دانش‌آموزان و آشنایی آنها با نمونه سئوالات امتحانی آورده شده است.

در پایان از کلیهٔ دست‌اندرکاران مجموعه ، بویژه **آقای اشراقی** مدیریت محترم انتشارات **صفار** تشکر می‌کنیم و پیشاپیش نظرات **منتقدان** و **یاریگران** را در جهت ارتقاء سطح کمی و کیفی مجموعه گرامی می‌داریم.



گروه آموزش مهارت
Gaam@Email.com

توانایی اول

آشنایی با برنامه‌های مخرب

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☑ برنامه‌های مخرب را تعریف نماید.
- ☑ انواع برنامه‌های مخرب را نام ببرد.
- ☑ راههای انتقال برنامه‌های مخرب را بداند.
- ☑ ویروس کامپیوتری را تعریف نماید.
- ☑ خواص ویروسهای کامپیوتری را نام ببرد.

زمان نظری : ۲ ساعت

زمان عملی : ----



۱-۱ آشنایی با برنامه‌های مخرب

هر نرم‌افزار با توجه به دستورالعمل‌هایی که در آن وجود دارد، عملیات خاصی را انجام می‌دهد. برنامه‌نویس یک نرم‌افزار با توجه به هدفی که از ایجاد نرم‌افزار دارد، یکسری دستورالعمل‌هایی را در نرم‌افزار پیشبینی می‌کند. حال اگر یک برنامه نویس قصد داشته باشد برنامه‌ای تولید کند که به برنامه‌های دیگر و فایلها و اطلاعات کامپیوتر آسیب برساند، یکسری دستورالعمل را جهت نابود کردن و یا خراب کردن فایل‌های کامپیوتر در نرم‌افزار قرار می‌دهد.

برنامه‌های مخرب با اهداف مختلفی تولید می‌شوند. گاهی اوقات یک برنامه مخرب جهت ضربه زدن به شرکتهای رقیب نرم‌افزاری و بدنام کردن محصولات شرکت رقیب تهیه می‌شود. گاهی اوقات برنامه مخرب توسط برنامه‌نویسان حرفه‌ای جهت ضربه زدن به اطلاعات شبکه‌های کامپیوتری کشورهای دیگر و یا نشان دادن قدرت نرم افزاری خود و مطرح کردن نام یک گروه در دنیای برنامه‌نویسان می‌باشد.

برنامه مخرب

برنامه‌هایی هستند که با هدف آسیب رساندن به نرم‌افزارهای دیگر و یا نابود کردن اطلاعات کامپیوتر تهیه می‌شوند.

۲-۱ انواع برنامه‌های مخرب

برنامه‌های مخرب از لحاظ نوع آسیب رسانی می‌توان به سه دسته زیر تقسیم کرد :

- **برنامه‌های مخرب نرم‌افزارها**

این برنامه‌ها برای ضربه زدن و نابود کردن یک نرم‌افزار مشخص یا محصولات یک شرکت خاص تولید می‌شوند.

- **برنامه‌های مخرب سخت‌افزارها**

این برنامه‌ها جهت آسیب رساندن به یک قطعه سخت‌افزاری نظیر مانیتور ، کارت گرافیک ، دیسک‌سخت ، آی‌سی **BIOS** و .... تهیه می‌شوند.

- **برنامه‌های مخرب اطلاعات**

این برنامه‌ها فقط به اطلاعات موجود در بانکهای اطلاعاتی آسیب می‌رساند.

- **برنامه‌های جاسوسی و نفوذ کننده**

این برنامه‌ها توسط نفوذگرها (**Hackers**) جهت نفوذ به شبکه‌های کامپیوتری ، کامپیوترهای شبکه ، کامپیوترهای شخصی و ... تهیه می‌شوند.

۱-۳ آشنایی با راههای انتقال برنامه‌های مخرب

برنامه‌های مخرب را همانند دیگر برنامه‌های کامپیوتری از طرق مختلفی می‌توان بر روی کامپیوترها منتقل کرد. ولی اگر دریافت کننده این برنامه بداند که ممکن است این برنامه مخرب باشد آن را اجرا نمی‌کند. به همین منظور تهیه کنندگان برنامه‌های مخرب ، سعی می‌کنند این برنامه‌ها را بدون اطلاع کاربران روی کامپیوتر آنها منتقل کرده و اجرا کنند و یا اینکه به روشهای مختلفی اطمینان کاربران کامپیوتر را جلب کنند و برنامه‌های مخرب را برنامه‌ای مفید و سودمند جلوه دهند.

۱-۴ آشنایی با مفهوم ویروس کامپیوتری

ویروس کامپیوتری به برنامه‌های مخرب کوچکی گفته می‌شود که مخفیانه وارد کامپیوتر می‌شوند و بدون اطلاع و اختیار کاربر خود را تکثیر می‌کنند. پس هر برنامه مخرب ، ویروس نیست. در واقع ویروس کامپیوتری نوعی برنامه‌مخرب است که خواص زیر را داشته باشد :

- **بسیار کوچک و کم حجم باشد**
- **بدون اطلاع کاربر بر روی کامپیوتر او منتقل شود**
- **بدون اطلاع کاربر تکثیر شده و به کامپیوترهای دیگر منتقل شود**

ویروس کامپیوتری

ویروس کامپیوتری به برنامه‌های مخرب کوچکی گفته می‌شود که مخفیانه وارد کامپیوتر می‌شوند و بدون اطلاع کاربر خود را تکثیر می‌کنند.

نام ویروس به این علت روی اینگونه از برنامه‌ها گذاشته شده است که عملکردی مشابهٔ ویروس‌های بیولوژیک دارند. یک ویروس بیولوژیک از طرق مختلفی ممکن است وارد بدن انسان شود و ممکن است تا مدّت زیادی به فعالیت مخفیانه در بدن بپردازد و پس از مدتی علائم وجود ویروس مشخص شود. یک ویروس کامپیوتری نیز از طرق مختلفی ممکن است وارد کامپیوتر شود و تا مدتها به فعالیت خود



ادامه دهد و پس از مدتی اختلالاتی را در کامپیوتر ایجاد نماید. ویروس‌های کامپیوتری می‌توانند به اطلاعات و برنامه‌های موجود در کامپیوتر آسیب رسانده و آنها را از بین ببرند.

ویروس‌های کامپیوتری توسط برنامه‌نویسان مجرب جهت آسیب رساندن به شرکتهای رقیب نرم‌افزاری، مختل کردن شبکه‌های کامپیوتری یا سایر مقاصد مشابه نوشته می‌شوند و همراه برنامه‌های قفل شکسته، برنامه‌های رایگان، از طریق اینترنت و غیره بِه کامپیوترهای دیگر انتقال می‌یابند.



۱ - برنامه‌های مخرب را تعریف نمایید.

۲ - انواع برنامه‌های مخرب را نام ببرید.

۳ - ویروس کامپیوتری را تعریف نمایید.

۴ - خواص ویروسهای کامپیوتری را نام ببرید.





۱- انواع برنامه‌های مخرب کدامند؟

الف) برنامه‌های مخرب نرم‌افزارها و سخت‌افزارها

ب) برنامه‌های مخرب اطلاعات و برنامه‌های جاسوسی و نفوذکننده‌ها

ج) برنامه‌های مخرب سخت‌افزارها

د) الف و ب

۲ - کدامیک خواص ویروس کامپیوتری نیست؟

الف) بسیار کوچک و کم حجم است.

ب) بدون اطلاع کاربر بر روی کامپیوتر او منتقل می‌شود.

ج) بدون اطلاع کاربر با قراردادن دو دیسک در کنار یکدیگر، از یک دیسک به دیسک دیگر منتقل می‌شود.

د) بدون اطلاع کاربر تکثیر شده و به کامپیوترهای دیگر منتقل می‌شود

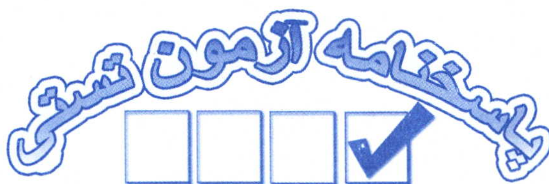
۳ - هدف از نوشتن ویروسهای کامپیوتری .... است.

الف) آسیب رساندن به شرکت‌های رقیب نرم‌افزاری

ب) مختل کردن شبکه‌های کامپیوتری

ج) آسیب رساندن به اینترنت

د) الف و ب



فصل	سئوال	الف	ب	ج	د
اول	۱				✓
	۲			✓	
	۳				✓

توانایی دوم

آشنایی با انواع ویروس

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☑ انواع ویروس از نظر محل تاثیر گذاری را نام ببرد.
- ☑ عملکرد ویروس‌های تاثیر گذار بر روی فایل‌های اجرایی را شرح دهد.
- ☑ عملکرد ویروس‌های تاثیر گذار بر روی فایل‌های غیر اجرایی را شرح دهد.
- ☑ عملکرد ویروس‌های تاثیر گذار بر رکورد راه‌انداز را شرح دهد.
- ☑ عملکرد ویروس‌های تاثیر گذار بر جدول Partition را شرح دهد.
- ☑ روش‌های انتقال ویروس به کامپیوتر را نام ببرد.

زمان نظری : ۱ ساعت

زمان عملی : -----

۲-۱ انواع ویروس از نظر محل تاثیر گذاری

ویروس‌ها مثل سایر برنامه‌های کامپیوتری نیاز به محلی برای ذخیرهٔ خود دارند، با این تفاوت که ویروسها محلی را انتخاب می‌کنند که برای رسیدن به اهداف شوم خود نزدیکتر و در دسترس تر باشند. محل‌هایی که برای جایگیری ویروس‌ها محبوبیت بیشتری دارند بشرح زیر می‌باشند :

- **فایلهای اجرایی**
- **فایلهای غیر اجرایی**
- **رکورد راه انداز (Boot Record)**
- **جدول پارتیشن (Partition Table یا Master Boot Record)**

در ادامه با انواع ویروسها از نظر محل تاثیر گذاری بیشتر آشنا خواهیم شد :

۲-۱-۱ ویروسهای تاثیرگذار بر روی فایلهای اجرایی

اکثر ویروس‌ها بطور انگل وار به فایلهای اجرایی می چسبند و آنها را آلوده می‌کنند تا پس از اجرا شدن آنها فعال شده و ضمن تکثیر خود، اطلاعات را از بین ببرند. به همین منظور اغلب نرم افزارهای ضد ویروس، فایلهای اجرایی یا انشعاب های زیر را بررسی یا پاکسازی می کنند :
.EXE ، .COM ، .SYS ، .BIN ، .OVL ، .DLL ، .SCR

بنابراین فایلهای اجرایی با انشعاب های فوق از اصلی‌ترین محل های جایگیری ویروسها می‌باشند.

۲-۱-۲ ویروسهای تاثیرگذار بر روی فایلهای غیر اجرایی

بندرت ویروسها در فایل های غیر اجرایی مثل فایل های متنی یا بانکهای اطلاعاتی جای می‌گیرند. از ویروسهای تاثیرگذار بر روی فایل‌های غیر اجرایی می‌توان به ویروسهایی اشاره کرد که در انتهای اسناد **Word** یا **Excel** خود را پنهان می‌کنند. این ویروسها بصورت دستورات نرم‌افزارهای **Word** یا **Excel** هستند که پس از باز شدن سند به صورت خودکار اجرا می‌شوند.
معمولاً آثار مخرب ویروسها بر روی فایلهای غیر اجرایی نمایان می‌شود و کمتر مشاهده شده است که ویروسها ، خود را در فایل‌های غیر اجرایی پنهان کنند.



۳-۱-۲ ویروسهای تاثیرگذار بر روی رکورد راه‌انداز (Boot Record)

برخی دیگر از ویروس ها علاقهٔ خاصی به پنهان شدن در رکورد راه‌انداز دارند زیرا رکورد راه انداز، واحد راه‌اندازی **DOS** است که در سکتور شمارهٔ صفر دیسک‌سخت یا فلاپی‌دیسک قرار دارد و اینگونه از ویروسها با قرار گرفتن در این محل به محض روشن شدن کامپیوتر و اجرای یک برنامه آلوده به ویروس و یا دسترسی به رکورد راه انداز ، همراه آن در حافظهٔ اصلی جا می گیرند و بعضی از آنها تا موقع خاموش شدن کامپیوتر همانجا باقی مانده و فایلهای دیگر را آلوده می کنند، حتی اگر برنامهٔ آلوده را حذف کرده یا فلاپی دیسک آلوده را نیز از دیسک گردان بیرون آورید.

رکورد راه‌انداز (Boot Record)

اولین سکتور یک دیسک است که در این سکتور توضیحاتی در مورد دیسک از قبیل سایز سکتورهای دیسک ، سایز کلاسترها و ... قرار دارد. علاوه بر این اطلاعات ، در دیسک‌های راه‌انداز این سکتور شامل برنامه‌ای است که سیستم عامل را در حافظه قرار داده و آن را راه‌اندازی می‌کند.

۴-۱-۲ ویروسهای تاثیرگذار بر روی جدول Partition

عملکرد ویروسهای تاثیرگذار بر روی جدول **Partition** همانند ویروسهای تاثیر گذار بر روی رکورد راه‌انداز هستند. این ویروس‌ها علاقه خاصی به پنهان شدن در جدول **Partition** دارند زیرا جدول **Partition** شامل اطلاعات تقسیم بندی دیسک سخت است که در سکتور شمارهٔ صفر دیسک سخت قرار دارد. اینگونه از ویروسها با قرار گرفتن در این محل به محض روشن شدن کامپیوتر و اجرای یک برنامه آلوده به ویروس و یا دسترسی به جدول **Partition** آلوده، همراه آن نرم‌افزار در حافظهٔ اصلی جا می‌گیرند و گاهی اوقات تا موقع خاموش شدن کامپیوتر همانجا باقی مانده و فایلهای دیگر را آلوده می‌کنند. همچنین ویروس‌هایی یافت می شوند که اطلاعات مربوط به **Setup** سیستم را نیز خراب کرده یا تغییر می‌دهند.

۲-۲ روشهای انتقال ویروس

ویروس‌های کامپیوتری ممکن است از راه‌های زیر به کامپیوتر انتقال یابند :

۱-۲-۲ انتقال ویروس از طریق دیسکت یا سی‌دی آلوده

بعضی از ویروس‌ها با چسبیدن به انتهای فایل‌های اجرایی (با پسوند **EXE** و **COM**) یا با قرار گرفتن روی سکتور دیسکت خود را به روی کامپیوتر منتقل می‌کنند. با اجرای فایل‌های آلوده یا با قرار دادن

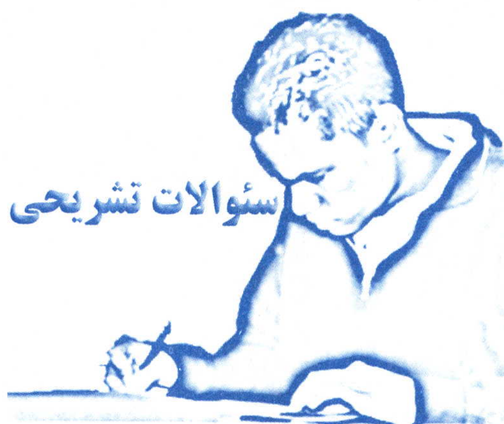
دیسکت آلوده در کامپیوتر و استفاده از آن، ویروس به کـامپیوتر منتقـل شـده و فعالیـت خـود را آغـاز می‌کند.

۲-۲-۲ انتقال ویروس از طریق شبکه

هرگاه یکی از کامپیوترهای متصل به شبکه آلوده به ویروس باشد، ممکن است ویروس از طریـق شـبکه همهٔ کامپیوترها را آلوده نماید. بعضی از ویروس‌ها مخصوص شبکه هسـتند و ابتـدا کـامپیوتر سـرویس دهنده (**Server**) را آلوده می‌کنند و سپس توسط کامپیوتر سرویس‌دهنده، کلیه کامپیوترهای شـبکه را آلوده می‌سازند.

۳-۲-۲ انتقال ویروس از طریق اینترنت

با گسترش استفاده از اینترنت، ویروس‌های اینترنتی به عنوان نسل جدیدی از ویروس‌ها مطرح شـدند. ویروس‌های اینترنتی بسیار سریعتر از ویروس‌های دیگر در سطح دنیا انتشار می‌یابند، به صورتیکه ظرف چند روز میلیونها کامپیوتر در سراسر دنیا به یک ویروس جدید آلوده مـی‌شـوند. ایـن نـوع ویـروس‌هـا ممکن است از طریق پست الکترونیک و یا از طریق دریافت فایل از اینترنت و ... بـه کـامپیوتر منتقـل شوند.



۱ - انواع ویروس از نظر محل تاثیر گذاری را نام ببرید.

۲ - عملکرد ویروس‌های تاثیر گذار بر روی فایل‌های اجرایی را شرح دهید.

۳ - عملکرد ویروس‌های تاثیر گذار بر روی فایل‌های غیر اجرایی را شرح دهید.

۴ - عملکرد ویروس‌های تاثیر گذار بر رکورد راه‌انداز را شرح دهید.

۵ - عملکرد ویروس‌های تاثیر گذار بر جدول Partition را شرح دهید.

۶ - روش‌های انتقال ویروس به کامپیوتر را نام ببرید.



۱- کدامیک از گزینه‌های زیر برای جایگیری ویروسها محبوب نیست؟

الف) فایل‌های اجرایی

ب) رکورد راه‌انداز و فایل‌های غیر اجرایی

ج) جدول راه‌انداز

د) جدول پارتیشن

۲ - انتقال .... از روش‌های انتقال ویروس می‌باشد.

الف) از طریق دیسک آلوده

ب) از طریق **CD** آلوده

ج) از طریق شبکه و اینترنت

د) هر سه گزینه

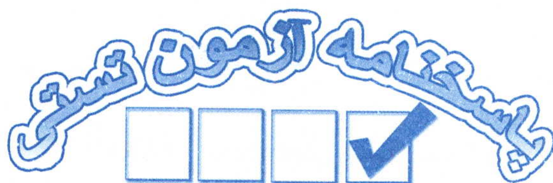
۳ - کدام یک از روش‌های انتقال، ویروس را سریعتر منتشر می کند؟

الف) از طریق اینترنت

ب) از طریق **CD** آلوده

ج) از طریق دیسک آلوده

د) از طریق شبکه



فصل	سئوال	الف	ب	ج	د
دوم	۱			✓	
	۲				✓
	۳	✓			

توانایی سوم

تشخیص ویروسی شدن سیستم

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☑ راههای تشخیص ویروسی شدن سیستم را نام ببرد.
- ☑ علائم ویروسی شدن سیستم را نام ببرد.
- ☑ کند شدن سیستم و دلایل آن شرح دهد.
- ☑ عدم راه‌اندازی سیستم و دلایل آن را شرح دهد.
- ☑ عدم اجرا شدن فایل‌های اجرایی و دلایل آن را شرح دهد.
- ☑ کند شدن ارتباط با اینترنت و دلایل آن را شرح دهد.

زمان نظری : ۱ ساعت

زمان عملی : ----



۱-۳ اصول تشخیص ویروسی شدن سیستم

ارائه روش دقیق و مشخصی برای تشخیص ویروسی بودن کامپیوتر امکان پذیر نیست اما از آنجاییکه همهٔ ویروس‌ها درصدد ایجاد مزاحمت و اختلال در کار کامپیوتر هستند و عملکرد همهٔ آنها منفی می‌باشد، لذا می‌توان از روی عملکرد آنها و عوارض ناشی از عملکرد آنها، ویروسی‌شدن سیستم را تشخیص داد. عملکرد ویروسها را که در واقع راههایی جهت تشخیص ویروسی‌شدن سیستم می باشند می‌توان بشرح زیر دسته بندی کرد :

- **ایجاد تاخیر، وقفه یا اختلال در عملیات راه اندازی کامپیوتر یا اجرای برنامه‌ها و فایلهای اجرایی.**
- **تخریب یا حذف اطلاعات و برنامه‌ها و یا حتی فرمت کردن دیسکها.**
- **اشغال حافظه و تکثیر در حافظه بطوریکه جایی برای اجرای برنامه های دیگر وجود نداشته باشد.**

مزاحمت‌ها و اختلال‌های فوق ممکن است به محض فعال شدن ویروس انجام شوند.

بطور کلی علائم زیر می‌تواند نشان‌دهنده ویروسی شدن کامپیوتر باشد :

۱-۱-۳ کند شدن سیستم

البته هر نوع کند شدن سیستم را نمی‌توان به ویروسها مرتبط کرد. کند شدن سیستم ممکن است به علت اجرای برنامه‌های متعدد، کم بودن حافظه اصلی کامپیوتر ، پایین بودن مشخصات کامپیوتر و ... باشد. ولی اگر کامپیوتر شما قبلاً با همین وضعیت سرعت مناسبی داشته و هم‌اکنون سرعت اجرای برنامه‌ها کم شده ، ممکن است سیستم شما ویروسی شده باشد.

۲-۱-۳ اشکال در راه‌اندازی سیستم

اگر هنگام راه‌اندازی کامپیوتر ، مشکلی پیش آید و کامپیوتر راه‌اندازی نشود، ممکن است کامپیوتر ویروسی شده باشد. معمولاً این ویروسها بر روی سکتور صفر دیسک سخت قرار می‌گیرند. بعضی از این ویروسها هنگام راه‌اندازی سیستم پیغامی را نمایش می‌دهند و به کاربر اعلام می‌کنند که کامپیوتر ویروسی است. یکی از این ویروسها ، ویروس **One Half** است که در هنگام راه‌اندازی کامپیوتر، عبارت زیر را نمایش می‌دهد :

This is One Half ...

۳-۱-۳ اشکال در اجرای فایلهای اجرایی

اگر فایل‌های اجرایی کامپیوتر، دچار مشکل شوند و اجرا نشوند ممکن است این فایل‌ها به ویروس آلوده شده باشند. گاهی اوقات وقتی یک فایل اجرایی به ویروس آلوده می‌شود، اندکی اندازه آن افزایش پیدا می‌کند. ولی ویروسهایی هم هستند که بدون آنکه اندازه یک فایل را تغییر دهند ، آن را آلوده می‌کنند.

۳-۱-۴ کند شدن ارتباط با اینترنت

بعضی از ویروسها ، اطلاعات کامپیوتر ما را بصورت مخفیانه از طریق اینترنت به نویسنده ویروس ارسال می‌کنند. بعضی از ویروسها ممکن است از طریق اینترنت خود را تکثیر کنند. یعنی پس از متصل شدن کامپیوتر به اینترنت شروع به تکثیر خود در اینترنت نمایند. بنابراین کند شدن ارتباط با اینترنت نیز می‌تواند یکی از دلایل ویروسی شدن کامپیوتر باشد.



۱ - راههای تشخیص ویروسی شدن سیستم را نام ببرید.

۲ - علائم ویروسی شدن سیستم را نام ببرید.

۳ - کند شدن سیستم و دلایل آن شرح دهید.

۴ - عدم راه‌اندازی سیستم و دلایل آن را شرح دهید.

۵ - عدم اجرا شدن فایل‌های اجرایی و دلایل آن را شرح دهید.

۶ - کند شدن ارتباط با اینترنت و دلایل آن را شرح دهید.



۱ - کدامیک از علائم زیر نشانه ویروسی شدن سیستم نیست؟

الف) ایجاد تاخیر، وقفه یا اختلال در عملیات راه اندازی کامپیوتر یا اجرای برنامه‌ها و فایلهـای اجرایی.

ب) توقف عملیات نرم‌افزار

ج) تخریب یا حذف اطلاعات و برنامه‌ها و یا حتی فرمت کردن دیسکها.

د) اشغال حافظه و تکثیر در حافظه بطوریکه جایی برای اجرای برنامه های دیگر وجود نداشته باشد.

۲ - کند شدن کامپیوتر از علائم ....

الف) اجرای برنامه‌های متعدد

ب) کم بودن حافظه اصلی کامپیوتر

ج) ویروسی شدن

د) هر سه مورد

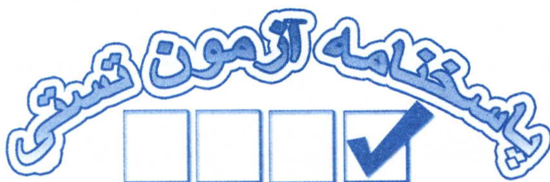
۳ - اگر هنگام راه‌اندازی کامپیوتر مشکلی پیش آید یا پیغامی نظیر **This is one Half** نمایش داده شود، نشانه چیست؟

الف) اجرای برنامه‌های متعدد

ب) کم بودن حافظه اصلی کامپیوتر

ج) ویروسی شدن

د) هر سه مورد



فصل	سئوال	الف	ب	ج	د
سوم	۱		✓		
	۲				✓
	۳			✓	

توانایی چهارم

مقابله با ویروسی شدن سیستم

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☑ روشهای مقابله با ویروسی شدن سیستم را نام ببرد.
- ☑ ویروس اینترنتی را شرح دهد.
- ☑ روش‌های انتشار ویروس‌های اینترنتی را نام ببرد.
- ☑ روشهای مقابله با ویروس‌های اینترنتی را شرح دهد.
- ☑ نحوه پاکسازی ویروس‌های مقیم در حافظه را شرح دهد.
- ☑ نحوه پاکسازی ویروس‌های غیر مقیم در حافظه را شرح دهد.
- ☑ نحوه پاکسازی ویروس‌های اینترنتی را شرح دهد.
- ☑ نرم‌افزار ضد ویروس را تعریف کند و با چند نمونه از آنها آشنا باشد.
- ☑ روش‌های مقابله نرم‌افزارهای ضد ویروس با ویروس‌ها را شرح دهد.

زمان نظری : ۲ ساعت

زمان عملی : ۴ ساعت



۱-۴ روشهای مقابله با ویروسها

در علوم پزشکی معروف است که پیشگیری آسانتر از درمان است در خصوص ویروسهای کامپیوتری نیز همین جمله کاملاً مصداق دارد، بطور کلی راههای اصلی مقابله و مبارزه با ویروسها به دو دستهٔ زیر تقسیم می شوند :

- **شناسائی ویروس ها و جلوگیری از ورود آنها به کامپیوتر (پیشگیری).**
- **از بین بردن ویروس های وارد شده به کامپیوتر و در صورت لزوم به وضعیت عادی بر گرداندن وضعیت سیستم (درمان).**

بعضی از راههای مقابله با ویروسی شدن سیستم عبارتند از :

- **ویروس‌ها هنگام ورود به سیستم به ناچار باید روی حافظه، برنامه و یا ناحیهٔ سیستمی دیسک قرار گیرند لذا معمولاً در سیستم یک حالت نوشتن اطلاعات بوجود می آید که این عمل تا حدودی قابل کنترل است. مثلاً با Write Protected کردن فلاپی دیسک یا Read Only کردن پارتیشن های دیسک می توان از نوشتن جلوگیری کرد. (پیشگیری)**
- **حتی‌المقدور از اتصال به کامپیوترها و شبکه‌هایی که از عدم ویروسی بودن آنها اطمینان ندارید بپرهیزید. (پیشگیری)**
- **هرگز از فلاپی دیسک‌هایی که از عدم ویروسی بودن آنها اطمینان ندارید استفاده نکنید. (پیشگیری)**
- **روی سیستم خود حتماً برنامه های ضد ویروسی که قابلیت مقیم شدن در حافظه را دارند قرار دهید. (پیشگیری)**
- **تنظیمات مربوط به کنترل ویروس را در Setup سیستم خود انجام دهید. (پیشگیری)**
- **وقتی ویروسی بر روی ناحیهٔ سیستمی دیسک یا بر روی فایل برنامه می نشیند، اندازه، تاریخ یا بعضی دیگر از مشخصات فایل اجرایی را تغییر می دهد. لذا می توان با تهیهٔ Backup های مرتب و مقایسه مشخصات فایلهای اجرایی و برنامه‌ها با نسخه‌های قبلی آنها از وجود احتمالی ویروس آگاهی پیدا کرد. (درمان)**

۲-۴ روشهای مقابله با ویروسهای اینترنتی

با گسترش شبکه اینترنت ، ویروسها راه مناسب و سریعتری را برای گسترش و تکثیر خود پیدا کردند بصورتی که اکثر ویروسهای امروزی از طریق اینترنت منتقل می‌شوند

ویروس اینترنتی

ویروس‌های اینترنتی به آن دسته از ویروس‌های کامپیوتری اطلاق می‌شود که از طریق اینترنت تکثیر یافته و منتقل می‌شوند.

ویروس‌های اینترنتی اغلب از طرق زیر وارد کامپیوتر می‌شوند:

- **انتقال از طریق نامه‌های الکترونیکی (E-mail)**

  به همراه نامه‌های الکترونیکی می‌توان فایل‌هایی را به صورت ضمیمه ارسال نمود. این فایل‌های ضمیمه ممکن است حاوی ویروس باشند. متأسفانه نامه‌های الکترونیکی بدون ضمیمه نیز می‌توانند حاوی ویروس باشند. به علت ضعف‌های امنیتی نرم‌افزارهای دریافت نامه‌های الکترونیکی نظیر نرم‌افزار **Outlook Express** ممکن است نامه‌های بدون ضمیمه نیز مخرب باشند. از معروفترین و خطرناکترین ویروس‌های اینترنتی که از طریق نامه‌های الکترونیکی انتقال می‌یابد، می‌توان به ویروس **NIMDA** اشاره کرد. این ویروس در عرض چند روز میلیونها کامپیوتر را در سراسر دنیا آلوده کرد و متأسفانه هنوز هم مواردی از آلودگی به این ویروس مشاهده می‌شود.

- **انتقال از طریق دریافت فایل آلوده از اینترنت**

  ممکن است در صفحات وب فوق متن دریافت فایلهای اجرایی وجود داشته باشد. که با کلیک کردن این فوق‌متن‌ها، یک فایل اجرایی و یا یک سند از طریق اینترنت دریافت شود. این فایلها ممکن است به ویروس‌ها آلوده باشند. در اینترنت سایتهایی وجود دارد که نرم‌افزارهای قفل شکسته را به صورت رایگان در اختیار افراد قرار می‌دهند. ممکن است این نرم‌افزارها آلوده به ویروس باشد.



بهترین راه مبارزه با ویروس‌های اینترنتی، پیشگیری از آلوده شدن به اینگونه ویروس‌هاست. برای جلوگیری از آلوده شدن به ویروسهای اینترنتی به توصیه‌های ساده اما مهم زیر توجه کنید :

- **نامه‌های الکترونیکی مشکوک را باز نکنید.**
- **ضمیمه‌های نامه‌های الکترونیکی ناشناس را باز نکنید.**
- **اگر ضمیمه نامه‌ها، فایلهای اجرایی یا اسناد نرم‌افزارهایی نظیر Microsoft Word بود بدون بررسی توسط نرم‌افزارهای ضد ویروس آنها را اجرا نکنید.**
- **فایل‌ها و برنامه‌هایی که از اینترنت دریافت می‌کنید، حتماً با نرم‌افزارهای ضد ویروس بررسی کرده و پس از اطمینان از سالم بودن فایل‌های دریافتی ، از آنها استفاده نمایید.**
- **نرم‌افزارهای ویروس یاب خود را به موقع بروز رسانی نمایید.**
- **سیستم‌عامل و نرم‌افزارهای اینترنتی خود را به موقع بروز رسانی نمایید.**
- **همواره از اخبار ویروس‌های جدید مطلع باشید. سایتهای مفیدی در این زمینه وجود دارند که آخرین اطلاعات ویروس‌های جدید را برای شما ارسال می‌کنند. این اطلاعات که به صورت نامه الکترونیکی برای شما ارسال می‌شود، حاوی اطلاعاتی در مورد نحوه شناسایی ویروس و فعالیتهای که ویروس انجام می‌دهد و نحوه حذف آن است. تعدادی از این سایتها عبارتند از:**

http://www.mcafee.com و http://www.antivirus.com/vinfo

۳-۴ آشنایی با مراحل پاکسازی سیستم آلوده

درصورتیکه به هر دلیلی کامپیوتر ما به ویروس آلوده شد ، باید هر چه سریعتر برای پاکسازی آن اقدام کنیم. برای پاکسازی ویروسها نمی‌توان یک روش مشخص را تعیین کرد زیرا هر ویروس عملکرد خاصی دارد که با توجه به نحوه تاثیرگذاری ویروس ، نوع ویروس ، نحوه آلوده کردن سیستم و ... باید روش مناسبی را جهت پاکسازی ویروس انتخاب کرد. ما در این قسمت پاکسازی ویروسها را به سه روش کلی توضیح می‌دهیم که هر روش برای پاکسازی ویروسهای خاصی کاربرد دارد.

۴-۳-۱ پاکسازی ویروسهای مقیم در حافظه

ویروسهای مقیم در حافظه، اغلب ویروسهایی هستند که بر روی رکورد راه‌انداز یا جدول **Partition** قرار دارند و در هنگام راه‌اندازی کامپیوتر فعال شده و در حافظه باقی می‌مانند. تا هنگامی که این ویروسها در حافظه قرار دارند، نمی‌توان برای پاکسازی آنها اقدام نمود.

جهت پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- ☑ *در صورت روشن بودن کامپیوتر، آن را مجدداً راه‌اندازی می‌نماییم.*
- ☑ *کامپیوتر را با یک دیسکت یا **CD** راه‌انداز سالم و عاری از ویروس ، راه‌اندازی می‌کنیم.*
- ☑ *دیسکت یا **CD** ضد ویروس مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.*
- ☑ *درصورتیکه سیستم عامل کامپیوتر آسیب دیده است و یا سیستم راه‌اندازی نمی‌شود می‌باید با توجه به نوع سیستم عامل ، عملیات بازسازی و احیاء سیستم عامل انجام شود.*

۴-۳-۲ پاکسازی ویروسهای غیر مقیم در حافظه

از آنجایی که این ویروسها در حافظه فعال نیستند، کافیست با نرم‌افزار ضدویروس مناسب آنها را پاکسازی نماییم.

جهت پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- ☑ *دیسکت یا **CD** ویروس یاب مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.*

۴-۳-۳ پاکسازی ویروسهایی اینترنتی

همانطور که می‌دانیم ویروسهای اینترنتی ، از طریق اینترنت به کامپیوتر منتقل می‌شوند. پس هنگام پاکسازی این ویروسها باید اتصال به اینترنت را قطع نمود زیرا ممکن است بلافاصله پس از پاکسازی ویروس، کامپیوتر مجدداً آلوده شود.

جهت پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- ☑ *ارتباط با اینترنت را قطع می‌کنیم.*
- ☑ *با توجه به دستورالعمل پاکسازی ویروس ، ممکن است نیاز باشد کامپیوتر را مجدداً راه‌اندازی می‌کنیم.*
- ☑ *دیسکت یا **CD** ضد ویروس مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.*



۴-۴ آشنایی با نرم‌افزارهای ضدویروس

یکی از روشهای جلوگیری از انتقال ویروس به کامپیوتر و حذف ویروسها از کامپیوتر استفاده از نرم‌افزارهای ضد ویروس است. نرم‌افزارهای ضد ویروس نرم‌افزارهایی هستند که فایلهای آلوده به ویروس را شناسایی کرده و ویروس را از روی کامپیوتر حذف می‌کنند.

همانطوریکه می دانید همه روزه ویروس های جدید با ساختار و عملکردهای مختلف توسط ویروس نویسان ساخته می شوند که شناسایی ساختار و عملکرد آنها و تهیهٔ برنامه‌های ضد ویروس مناسب آنها، مستلزم صرف هزینه و وقت نسبتاً زیادی است. به همین دلیل تهیهٔ ضد ویروس مناسب هر ویروس، براحتی امکان پذیر نیست و هیچ شرکت تولید کنندهٔ برنامه های ضد ویروس، نمی تواند ادعا نماید که قادر به شناسائی و از بین بردن تمام ویروس‌ها می باشند و تا زمانیکه ضد ویروس یک ویروس جدید طراحی می گردد ممکن است کامپیوترهای زیادی آلوده و دچار اختلال گردند.

از معروفترین و متداولترین نرم‌افزارهای ضد ویروس می‌توان به نرم‌افزارهای زیر اشاره کرد:

- **McAfee Virus Scan**
- **Norton Antivirus**
- **Panda Antivirus**
- **Dr Web**

نرم‌افزارهای ضد ویروس فقط می‌توانند ویروسهای شناخته شده را تشخیص دهند و قادر نیستند ویروسهای جدید را تشخیص دهند. برای حل این مشکل ، در نرم‌افزارهای ضد ویروس امکان بروز رسانی در نظر گرفته شده است به صورتیکه از طریق اینترنت می‌توان نرم‌افزار ضد ویروس را بروز رسانی کرد. شرکتهای تولید کننده نرم‌افزارهای ضد ویروس جدیدترین ویروسها را شناسایی کرده و فایل‌های بروز رسانی نرم‌افزار ضد ویروس خود را در سایت وب قرار می‌دهند تا مشترکین آنها در سراسر دنیا نرم‌افزارهای خود را بروز رسانی نمایند.

۵-۴ روشهای مقابله نرم‌افزارهای ضدویروس با ویروسها

نرم‌افزارهای ضد ویروس به روش‌های زیر با ویروسها مقابله می‌کنند :

- **پیشگیری از آلوده شدن به ویروس**

در هنگام وارد شدن ویروس به کامپیوتر ، پیغام هشدار دهنده‌ای را به کاربر نمایش می‌دهند و از فعال شدن ویروس خودداری می‌کنند.

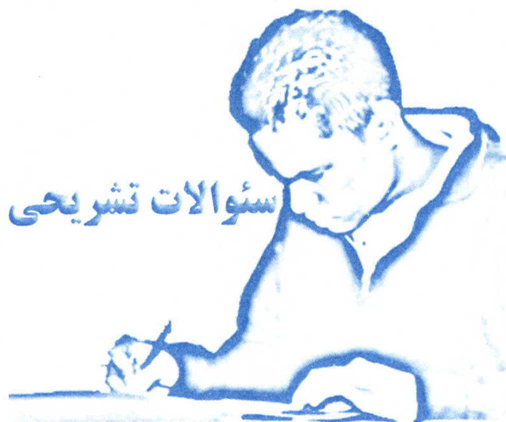
- **پاک کردن ویروس**

فایلهای سالمی که به ویروس آلوده شده اند را شناسایی می‌کنند و در صـورت امکـان آنهـا را ویروس‌زدایی کرده و به صورت اولیه باز می‌گردانند به این عمل **disinfecting** (ویروس‌زدایی) می‌گویند.

- **قرنطینه کردن فایل ویروسی**

درصورتیکه نتوانند یک فایل‌آلوده را ویروس‌زدایی کنند آن فایل را قرنطینه کرده و بـه کـاربر اطلاع می‌دهند که این فایل آلوده به ویروس است و امکان ویروس زدایی آن نیست و فعلاً در قرنطینه است. درصورتیکه کاربر مایل باشد می‌تواند این فایل را به کلی حذف کند. همچنـین نرم‌افزارهای ضدویروس به کاربران اجازه می‌دهند، فایل‌های مشکوک را بـه قسـمت قرنطینـه منتقل کنند.





۱ - روشهای مقابله با ویروسی شدن سیستم را نام ببرید.

۲ - ویروس اینترنتی را شرح دهید.

۳ - روش‌های انتشار ویروس‌های اینترنتی را نام ببرید.

۴ - روشهای مقابله با ویروس‌های اینترنتی را شرح دهید.

۵ - نحوه پاکسازی ویروس‌های مقیم در حافظه را شرح دهید.

۶ - نحوه پاکسازی ویروس‌های غیر مقیم در حافظه را شرح دهید.

۷ - نحوه پاکسازی ویروس‌های اینترنتی را شرح دهید.

۸ - نرم‌افزار ضد ویروس را تعریف کرده و چند نمونه از آنها را نام ببرید.

۹ - روش‌های مقابله نرم‌افزارهای ضد ویروس با ویروس‌ها را شرح دهید.



۱ - کدامیک از موارد زیر، پیشگیری از ویروسی شدن کامپیوتر می‌باشد.

الف) شناسایی ویروس و جلوگیری از ورود آن به کامپیوتر

ب) از بین بردن ویروس وارد شده به کامپیوتر

ج) عدم اتصال به اینترنت

د) هر سه گزینه

۲ - برای جلوگیری از ویروسی شدن کامپیوتر چه کاری را باید انجام داد؟

الف) **Write Protected** کردن فلاپی دیسک

ب) عدم اتصال به کامپیوترها و شبکه‌های ناشناخته

ج) عدم استفاده از فلاپی دیسک‌های ناشناخته

د) هر سه گزینه

۳ - ویروسهای .... از طریق نامه‌های الکترونیکی وارد کامپیوتر می‌شوند.

الف) اینترنتی　　**ب)** سیستمی

ج) مخرب　　**د)** مقیم در حافظه

۴ - برای جلوگیری از آلوده شدن به ویروسهای اینترنتی کدامیک از روش‌های زیر موثر است؟

الف) باز نکردن نامه‌های الکترونیکی مشکوک

ب) بروزرسانی نرم‌افزار ویروس‌یاب

ج) بروزرسانی سیستم عامل

د) هر سه مورد



۵ - کدامیک از سایتهای زیر مربوط به برنامه‌های ضد ویروس می‌باشند؟

الف) http://www.mcafee.com **ب)** http://www.antivirus.com

ج) http://www.google.com **د)** الف و ب

۶ - روش‌های مقابله نرم‌افزارهای ضدویروس با ویروس‌ها .... است.

الف) پیشگیری از آلوده شدن به ویروس

ب) پاک کردن ویروس

ج) قرنطینه کردن فایل ویروسی

د) هر سه مورد

۷ - درصورتیکه دیسکتی که احتمالا حاوی ویروس است به شما داده شده است و شما نیاز دارید که از این دیسکت استفاده نمایید ، برای اینکه کامپیوتر شما ویروسی نشود چه کاری باید بکنید؟

الف) دیسکت را فرمت می‌کنیم.

ب) ابتدا دیسکت را ویروس‌یابی کرده و پس از حذف ویروس‌ها از آن استفاده می‌کنیم.

ج) ابتدا دیسکت را **Write Protect** کرده و پس از حذف ویروس‌ها از آن استفاده می‌کنیم.

د) گزینه‌های ب و ج

۸ - فرض کنید که بر روی یک دیسکت چند فایل قرار داده‌اید و می‌خواهید این فایل‌ها را در کامپیوتر دوست خود کپی کنید. با توجه به اینکه کامپیوتر دوست شما ممکن است ویروسی باشد چه کاری باید انجام دهید تا دیسکت شما ویروسی نشود؟

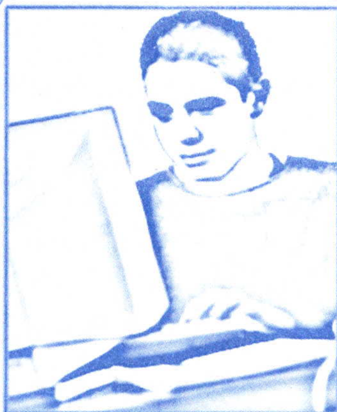
الف) دیسکت را فرمت می‌کنیم.

ب) ابتدا دیسکت را از حالت **Write Protect** خارج کرده و سپس آن را در درایو کامپیوتر قرار می‌دهیم.

ج) ابتدا دیسکت را در حالت **Write Protect** قرار داده و سپس آن را در درایو کامپیوتر قرار می‌دهیم.

د) هیچکدام

دستور کار آزمایشگاه



۱ - از طریق اینترنت به سایت **http://www.mcafee.com** متصل شوید و اطلاعاتی در مورد نرم‌افزار ضد ویروس **McAfee** بدست آورید.

۲ - از طریق اینترنت به سایت **http://www.antivirus.com** متصل شوید و اطلاعاتی در مورد ویروس‌های جدید اینترنتی بدست آورید.

۳ - به سایت متصل شوید . در این سایت اطلاعاتی در مورد ویروس‌های اینترنتی به زبان فارسی وجود دارد. نحوه عملکرد و نحوه مقابله با ویروس‌های **Nimda** ، **Sircam** ، **Code Red** را بدست آورید.

۴ - عملیات پاکسازی ویروس‌های مقیم در حافظه را یکبار تمرین کنید.

۵ - عملیات پاکسازی ویروس‌های غیرمقیم در حافظه را یکبار تمرین کنید.

۶ - عملیات پاکسازی ویروس‌های اینترنتی را یکبار تمرین کنید.



فصل	سئوال	الف	ب	ج	د
چهارم	۱	✓			
	۲				✓
	۳	✓			
	۴				✓
	۵				✓
	۶				✓
	۷		✓		
	۸			✓	

توانایی پنجم

کار با نرم‌افزار ضد ویروس McAfee

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☑ نرم‌افزار McAfee را نصب نماید.
- ☑ قسمتهای مختلف نرم‌افزار McAfee را نام برده و کاربرد هر یک را توضیح دهد.
- ☑ عملیات ویروس‌یابی را به کمک نرم‌افزار McAfee انجام دهد.
- ☑ نرم‌افزار McAfee را از طریق اینترنت بروزرسانی نماید.

زمان نظری : -----

زمان عملی : ۴ ساعت

۵-۱ آشنایی با نرم‌افزار McAfee

با ادغام دو شرکت **Dr Solomon's Software** (تولیدکننده نرم‌افزارهای ضد ویروس **Toolkit**) و شرکت **Network Associates** (تولیدکننده نرم‌افزارهای ضد ویروس **McAfee**) نسل جدیدی از نرم‌افزارهای پیشرفته ضد ویروس به بازار عرضه شد. در واقع ضد ویروس **McAfee** ترکیبی از قدرت شناسایی و پاکسازی **Toolkit** و راحتی استفاده **McAfee** است. هم اکنون ضد ویروس **McAfee** بیش از ۷۰ میلیون کاربر در سطح دنیا دارد و در حدود ۵۶٪ بازار نرم‌افزارهای ضد ویروس در اختیار این ضد ویروس است. از مهمترین مزایای این ضد ویروس، به روزرسانی ساده و سریع آن است. ما در این کتاب نسخه **2004** نرم‌افزار **McAfee** را توضیح خواهیم داد. با نحوه نصب و استفاده از این نرم افزار در ادامه همین فصل آشنا می شویم.

۵-۲ نصب نرم‌افزار McAfee

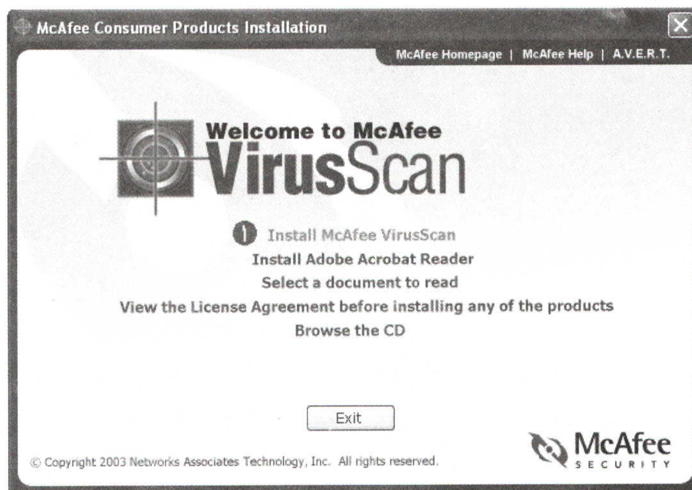
جهت نصب نرم‌افزار **McAfee** عملیات زیر را انجام می‌دهیم :

☑ ***CD*** *نصب نرم‌افزار* ***McAfee*** *را در درایو قرار داده و فایل* ***Setup.exe*** *را اجرا می‌کنیم.*



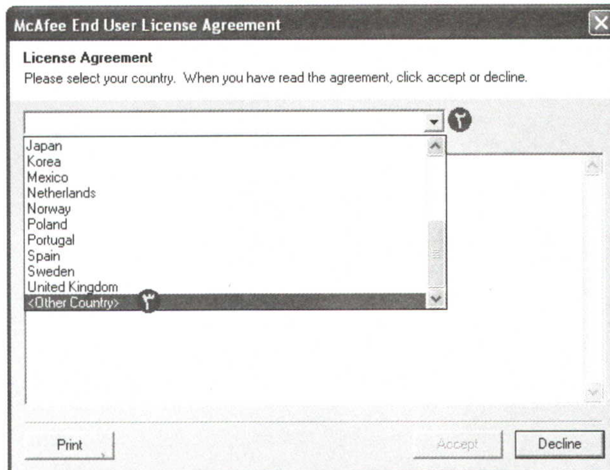
شکل (۱-۵) آیکن برنامه **Setup** نرم‌افزار **McAfee**

☑ *پنجره‌ای مطابق شکل زیر ظاهر می‌شود. در این پنجره بر روی* ***Install McAfee VirusScan*** *کلیک می‌کنیم.*



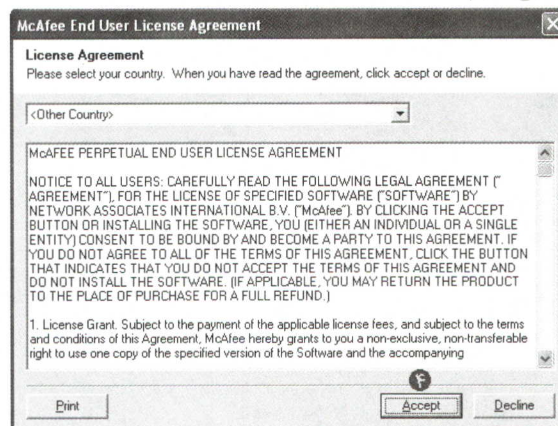
شکل (۲-۵) پنجره نصب ضدویروس **McAfee**

☑ پنجره‌ای مطابق شکل زیر ظاهر می‌شود. در این پنجره از لیست **Country** ، نام کشور خود را انتخاب می‌کنیم. از آنجایی که کشور ایران در این لیست وجود ندارد، گزینه **Other Country** را انتخاب می‌نماییم.



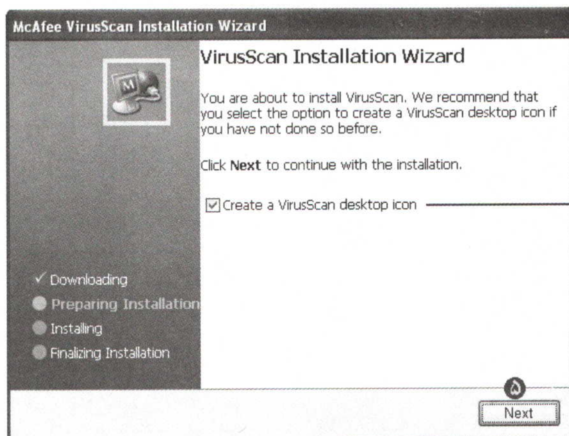
شکل (۳-۵) انتخاب نام کشور – پنجره **User License Agreement**

☑ متن موافقتنامه مجوز استفاده از نرم‌افزار ظاهر می‌شود. بر روی دکمه Accept جهت قبول این موافقت نامه کلیک می‌کنیم.



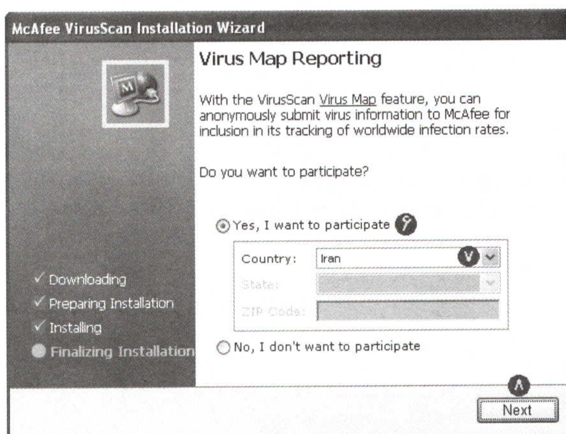
شکل (۴-۵) نمایش متن موافقتنامه مجوز کاربر نهایی

☑ پنجره **VirusScan Installation Wizard** ظاهر می‌شود. در این پنجره می‌توانیم مشخص نماییم که آیکن میانبر برنامه **VirusScan** بر روی میزکار قرار گیرد یا خیر. جهت ادامه کار بر روی دکمه Next > کلیک می‌کنیم.



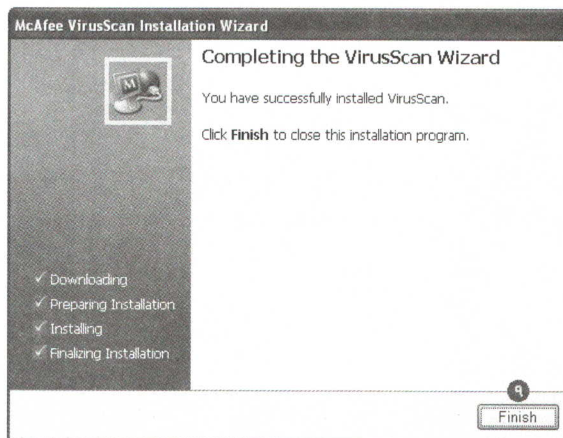
شکل (۵-۵) پنجره **VirusScan Installation Wizard**

☑ در مرحله بعد ، برنامه نصب فایل‌های لازم را بر روی دیسک کپی می‌کند. سپس پنجره زیر ظاهر می‌شود. در این پنجره جهت اشتراک داوطلبانه در قسمت **Virus Map** سایت **McAfee** از ما سئوال می‌شود. به کمک امکان **Virus Map** می‌توان اطلاعات ویروسهای کامپیوتر ما را به صورت ناشناس به شرکت **McAfee** ارسال نمود تا این شرکت بتواند نرخ ابتلا به یک ویروس را در سطح جهان اندازه‌گیری نماید و آمار کامپیوترهای مبتلا به یک ویروس را در سطح جهان منتشر نماید. در صورتیکه بخواهیم در **Virus Map** مشترک شویم ، گزینه Yes, I want to participate را انتخاب کرده و نام کشور **Iran** را از لیست انتخاب می‌نماییم. سپس دکمه Next > را کلیک می‌کنیم.



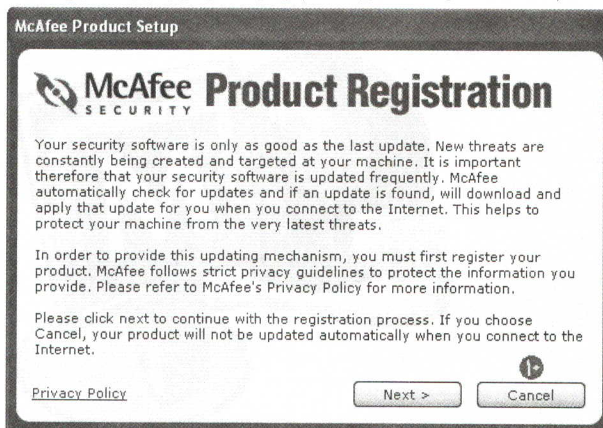
شکل (۶-۵) پنجره **Virus Map Reporting**

☑ در پنجره بعد دکمه Finish را کلیک می‌کنیم تا عملیات نصب به پایان برسد.



شکل (۵-۷) پنجره **Completing the VirusScan Wizard**

☑ *پس از این پنجره ، پنجره **Register** کردن نرم‌افزار **VirusScan** ظاهر می‌شود. درصورتیکه بخواهیم این پنجره را ببندیم، دکمه Cancel را کلیک می‌کنیم. (درصورتیکه بخواهیم نرم‌افزار خود را **Register** کنیم باید به اینترنت متصل باشیم و در ضمن نرم‌افزار ما کپی غیرمجاز نباشد.)*



شکل (۵-۸) پنجره **McAfee Product Registration**

۵-۳ آشنایی با محیط کار نرم‌افزار McAfee

جهت اجرای نرم‌افزار **McAfee** بر روی آیکن M که در سینی نوار کار قرار دارد، دوبار کلیک می‌کنیم.



شکل (۵-۹) آیکن نرم‌افزار ضد ویروس **McAfee** در نوار کار ویندوز

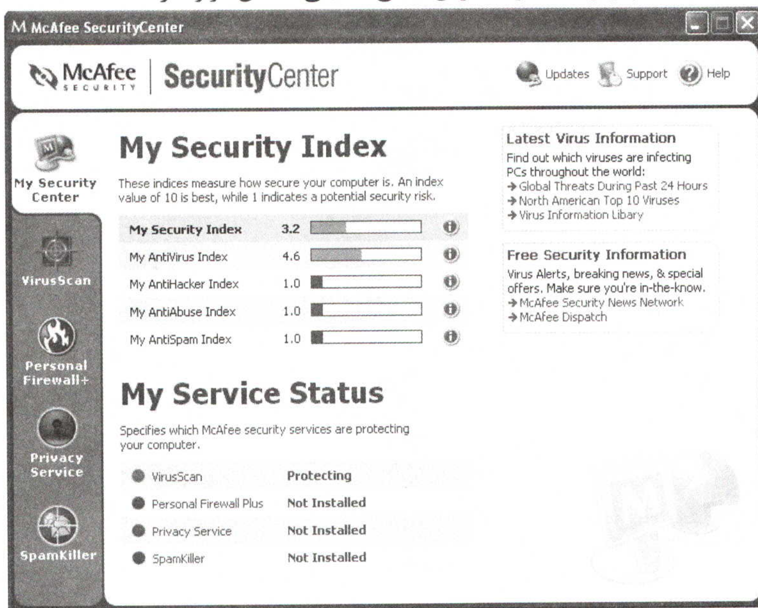
پنجره اصلی برنامه **McAfee** ظاهر می‌شود. این پنجره شامل چندین سربرگ است که هر سربرگ یک نرم‌افزار جداگانه محسوب می‌شود.

هنگامی که نرم‌افزار **McAfee** را نصب می‌کنیم، فقط قسمت **Virus Scan** نصب می‌شود. در ادامه با عملکرد هر یک از سربرگ‌های نرم‌افزار **McAfee** آشنا خواهیم شد.

۱-۳-۵ مرکز امنیت من



در این سربرگ قسمتی تحت عنوان **My Security Index** وجود دارد ، که در این قسمت ضرایبی نمایش داده می‌شود که هر ضریب نشان دهنده میزان امنیت کامپیوتر شما در یک زمینه است. اگر این ضریب یک باشد به این معنی است که امنیت کامپیوتر شما در این موضوع پایین است. ضریب ۱۰ نمایانگر این است که کامپیوتر شما در بالاترین سطح امنیتی ممکن قرار دارد.



شکل (۱۰-۵) سربرگ **My Security Center** نرم‌افزار **McAfee**

همانطور که در قسمت **My Service Status** شکل فوق مشاهده می‌شود ، سرویس‌های **Personal Firewall** ، سرویس **Privacy Service** و **Spam Killer** بر روی کامپیوتر نصب نشده است. بنابراین ضریب امنیتی این کامپیوتر در این مواد پایین است.

در صورتیکه می‌خواهید ضریب امنیتی کامپیوتر شما در همه زمینه‌ها بالاتر بـرود بایـد کارهـای زیـر را انجام دهید:

☑ *نرم‌افزار **Virus Scan** خود را از طریق اینترنت بروز کنید.*
☑ *نرم‌افزار **Personal Firewall** شرکت **McAfee** را نصب نمایید.*
☑ *سرویس **Privacy Service** شرکت **MacAfee** را فعال نمایید.*
☑ *نرم‌افزار **Spam Killer** شرکت **McAfee** را نصب نمایید.*

با این نرم‌افزارها در ادامه بیشتر آشنا خواهیم شد.

۲-۳-۵ سربرگ ویروس‌یابی 

در این سربرگ قسمتهای مختلفی وجود دارد. این قسمتها عبارتند از :

- **ویروس‌یابی کامپیوتر من** Scan My Computer for Viruses

ویروس‌یابی کامپیوتر و حذف ویروسها از طریق این گزینه انجام می‌گردد.

- **تنظیمات ویروس‌یابی** Configure VirusScan Options

تنظیمات نرم‌افزار ویروس‌یاب از طریق این گزینه انجام می‌شود.

- **مدیریت فایل‌های قرنطینه شده** Manage Quarantined Files

قرنطینه کردن برنامه‌ها و اسنادی که تصور می‌کنیم ممکن است ویروسی باشند از طریق ایـن گزینه انجام می‌شود.

- **مشاهده نقشه جهانی ویروسها** View the World Virus Map

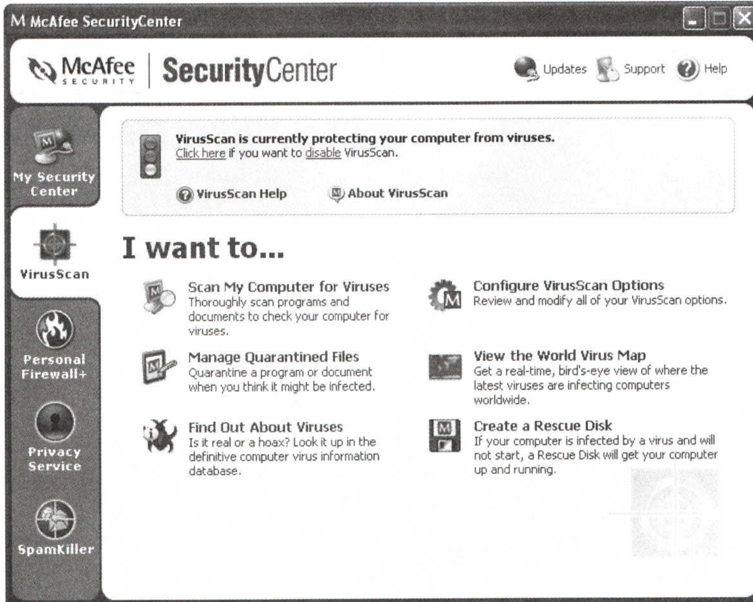
نرم‌افزار **McAfee** اطلاعات آماری ویروسهای مشاهده شده در سراسر جهان را بـر روی نقشـه از طریق این گزینه در اختیار شما قرار می‌دهد.

- **جستجوی اطلاعات ویروسها** Find Out About Viruses

در این قسمت می‌توانید اطلاعات کاملی در مورد ویروسهای شناخته شده و نحـوه عملکـرد و پاکسازی آنها بدست آورید.

- **ایجاد دیسک نجات**  Create a Rescue Disk

این قسمت یک دیسک نجات برای شما می‌سازد. درصورتیکه کامپیوتر شما ویروسی شود و دیگر راه‌اندازی نشود، به کمک دیسک نجات می‌توانید کامپیوتر خود را راه‌اندازی نمایید.



شکل (۱۱-۵) سربرگ **VirusScan** نرم‌افزار **McAfee**

۵-۳-۳ سربرگ دیوار آتش شخصی



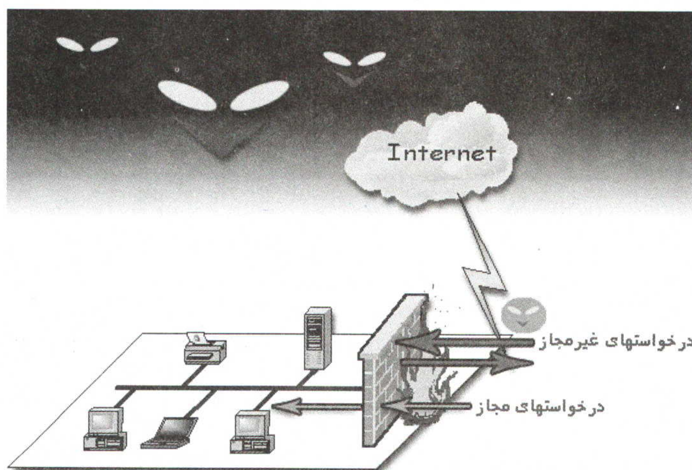
یکی از خطراتی که کامپیوترهای متصل به شبکه‌های کامپیوتری و شبکه اینترنت را تهدید می‌کند ، خطر نفوذ افرادی به نام نفوذگر (**Hacker**) می‌باشد. نفوذگرها افرادی هستند که از طریق سوراخهای امنیتی موجود در سیستم‌عامل یا نرم‌افزارهای دیگر، به کامپیوتر شما نفوذ کرده و علاوه بر اینکه می‌توانند اطلاعات محرمانه شما را به سرقت ببرند، می‌توانند آسیبهای جدی به فایل‌ها و برنامه‌های شما وارد نمایند. در گذشته، نفوذگرها ، افراد حرفه‌ای و مسلط به کامپیوتر بودند که معمولاً به کامپیوترهای شرکتهای بزرگ و مراکز حساس نفوذ می‌کردند و کمتر در فکر نفوذ به کامپیوترهای شخصی بودند ولی امروزه با ابزارهای جاسوسی که در سایتهای اینترنتی مخصوص نفوذگرها به رایگان قابل دریافت است، کاربران تازه کار نیز با استفاده از این ابزارها می‌توانند به راحتی به کامپیوترها نفوذ کنند، بنابراین خطر نفوذ به کامپیوترهای شخصی به مراتب بیشتر شده است. به همین منظور

شرکتهای تولید کننده نرم‌افزارهای ضدویروس، به همراه نرم‌افزار ضدویروس خود نرم‌افزاری به نام دیوار آتش (**Firewall**) نیز ارائه می‌کنند که این نرم‌افزار مراقبت از کامپیوتر شما در برابر نفوذگرها را به عهده دارد. در گذشته دیوارهای آتش توسط مدیران شبکه و مسئولین **ISP** بر روی کامپیوترهای **Server** نصب می‌شد ولی امروزه نوع ساده‌تری از دیوارهای آتش تولید شده‌اند که به آنها دیوار آتش شخصی (**Personal Firewall**) می‌گویند.

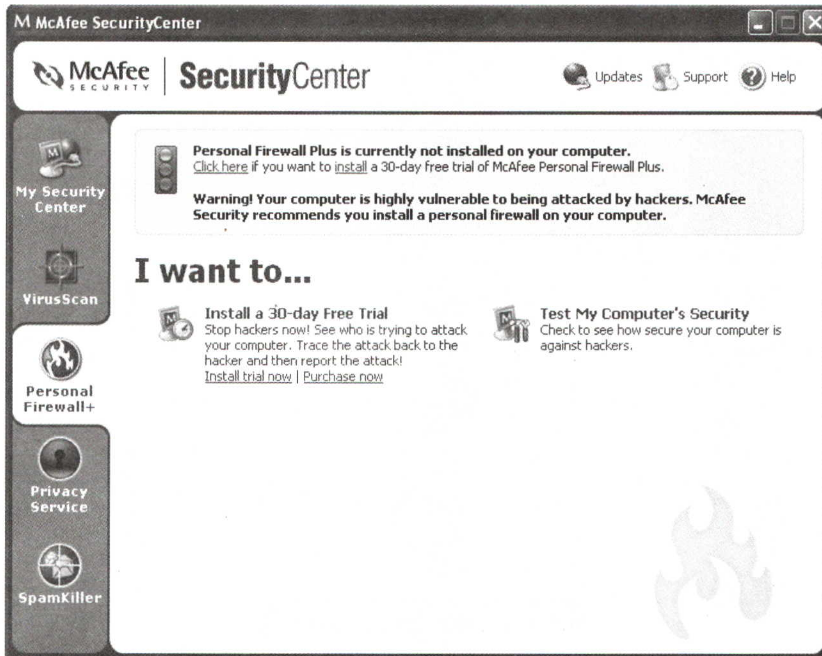
دیوار آتش (Firewall)

سیستم امنیتی را که جهت محافظت از شبکه داخلی در مقابل نفوذ افراد از خارج شبکه طراحی شده است ، اصطلاحاً دیوار آتش می‌گویند.

همانطور که در شکل زیر مشاهده می‌کنید، دیوار آتش به درخواستهای مجاز اجازه عبور می‌دهد ولی درخواستهای غیر مجاز را بازمی‌گرداند و به این ترتیب از نفوذ افراد غیر مجاز جلوگیری می‌کند.



شکل (۱۲-۵) دیوار آتش به درخواستهای مجاز اجازه عبور می‌دهد ولی درخواستهای غیر مجاز را بازمی‌گرداند.



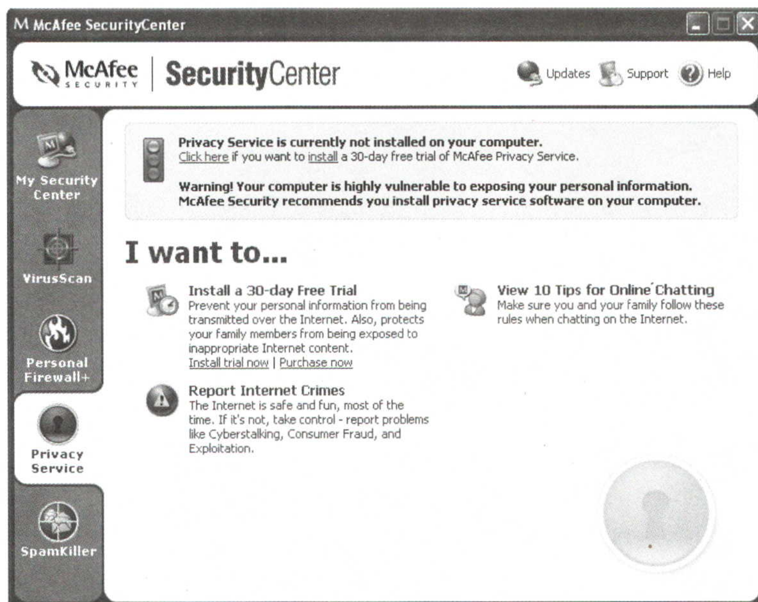
شکل (۱۳-۵) سربرگ **Personal Firewall** نرم‌افزار **McAfee**

همانطور که در شکل مشاهده می‌کنیم نرم‌افزار دیوار آتش شخصی ، نصب نشده است و برای نصب آن باید بر روی Install a 30-day Free Trial کلیک کنیم تا از طریق اینترنت ، نسخه آزمایشی ۳۰ روزه آن بر روی کامپیوتر ما نصب شود.

۴-۳-۵ سربرگ سرویس اختفاء



در این سربرگ ، نرم‌افزار **McAfee** سرویس دیگری را به نام سرویس اختفاء در اختیار کاربران خود قرار می‌دهد. این سرویس از انتشار اطلاعات شخصی شما در شبکه اینترنت جلوگیری می‌کند. همچنین توسط این سرویس می‌توان قوانینی را وضع نمود که دسترسی به سایتهای غیر مجاز غیر ممکن شود.

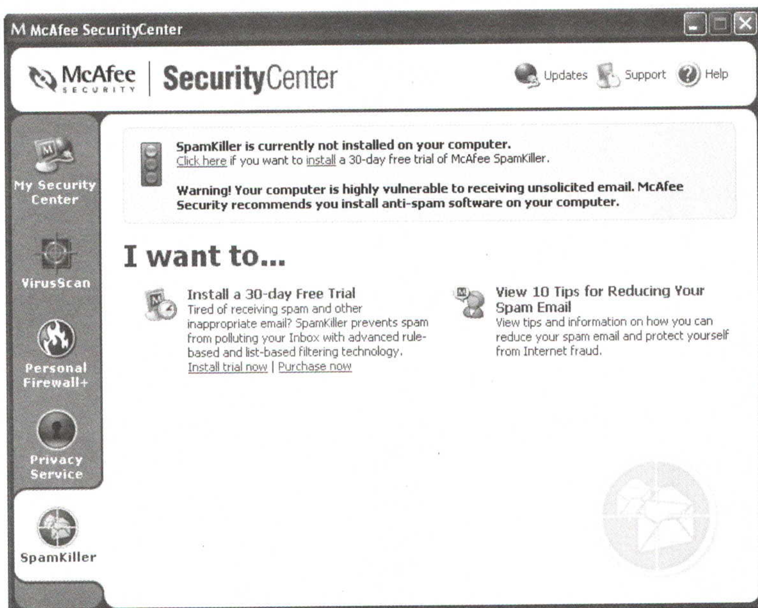


شکل (۱۴-۵) سربرگ **Privacy Service**

۵-۳-۵ سربرگ نابودکننده هرز نامه 

یکی از مشکلاتی که کاربران اینترنتی با آن مواجه هستند، ارسال نامه‌های الکترونیکی زیاد بصورت ناخواسته و معمولاً با محتوای تبلیغاتی است که باعث می‌شود صندوق پستی الکترونیکی افراد مملو از این نامه‌ها شود. به اینگونه نامه‌ها هرزنامه (**Spam**) گفته می‌شود.

در این سربرگ ، امکان نصب نسخه آزمایشی ۳۰ روزه نرم‌افزار **SpamKiller** قرار داده شده است. این نرم‌افزار نامه‌های **Spam** را تشخیص داده و از صندوق پست الکترونیک شما حذف می‌کند. در این نرم‌افزار می‌توان قوانینی را وضع کرد که نامه‌های خاصی را به عنوان **Spam** شناسایی کرده و حذف نماید.



شکل (۱۵-۵) سربرگ **SpamKiller** نرم‌افزار **McAfee**

۴-۵ ویروس‌یابی با نرم‌افزار McAfee

پس از نصب نرم‌افزار **McAfee** ، این نرم‌افزار بصورت مقیم در حافظه قرار می‌گیرد. در ضمن هربار که کامپیوتر را روشن کنیم این نرم‌افزار به صورت خودکار اجرا شده و در حافظه قرار می‌گیرد. هر فایل یا پوشه‌ای را که باز کنیم، نرم‌افزار **McAfee** بصورت خودکار فایل‌های داخل آن را پوشه را بررسی می‌کند و درصورتیکه فایل ویروسی پیدا کند بلافاصله پیغامی را نمایش می‌دهد و از فعالیت ویروس جلوگیری می‌کند.

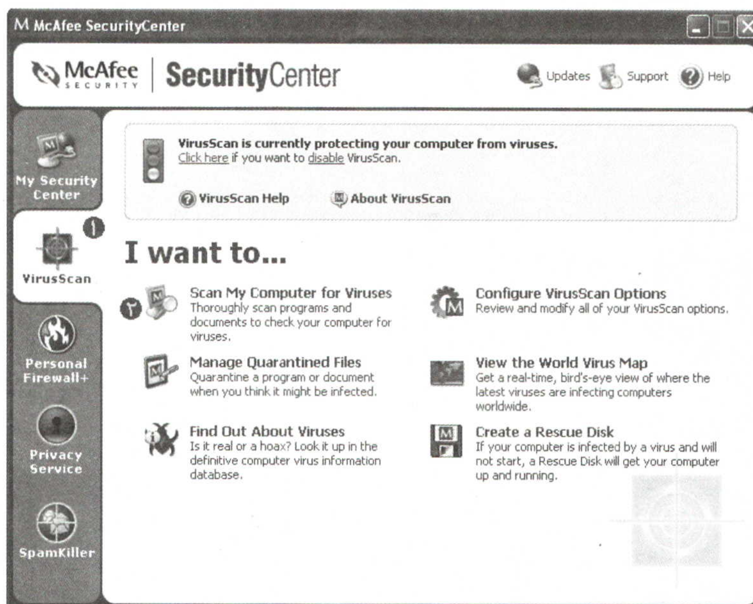
گاهی اوقات ممکن است بخواهیم تمام یا بخشی از فایل‌های کامپیوتر را ویروس‌یابی کنیم.

برای ویروس‌یابی کامپیوتر عملیات زیر را انجام می‌دهیم :

☑ *بر روی آیکن M در سینی نوار کار، دوبار کلیک می‌کنیم.*

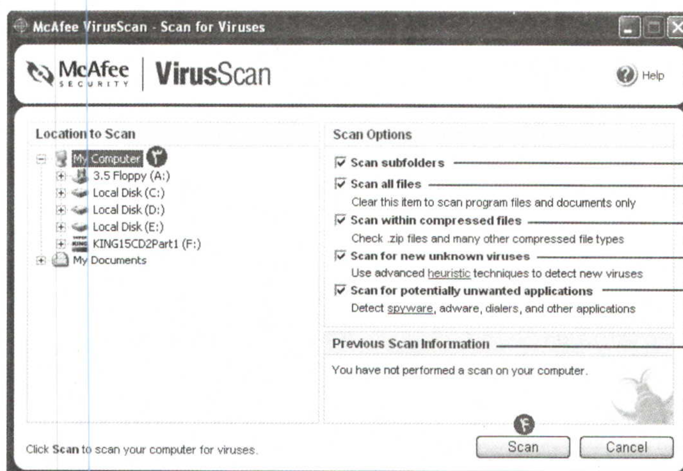
☑ *در پنجره برنامه **McAfee** ، روی سربرگ VirusScan کلیک می‌کنیم.*

☑ *در این سربرگ ، بر روی Scan My Computer for Viruses کلیک می‌کنیم.*



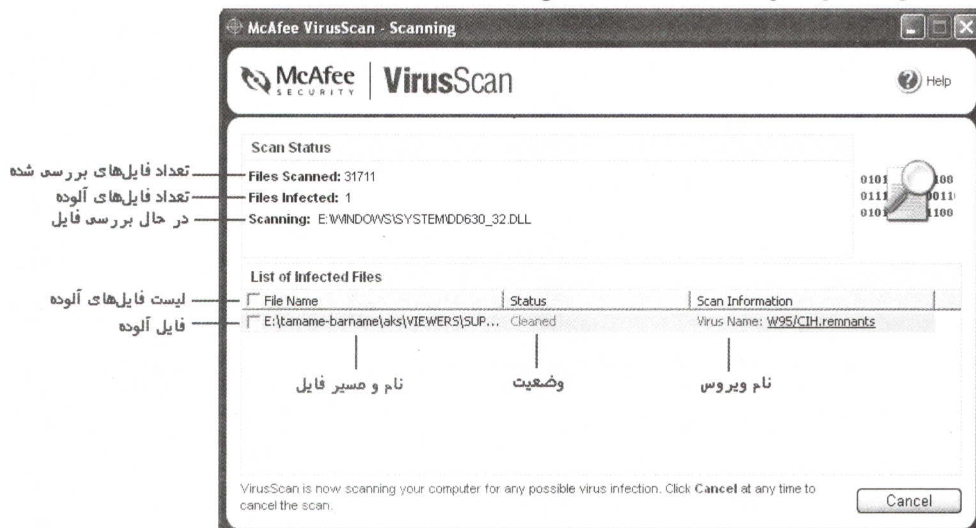
شکل (۵-۱۶) سربرگ **VirusScan** نرم‌افزار **McAfee**

☑ *در پنجره ظاهر شده، درایو یا پوشه مورد نظر را جهت ویروس‌یابی انتخاب می‌کنیم. همچنین در قسمت **Scan Options** می‌توان تعیین نمود چگونه ویروس‌یابی انجام شود.*



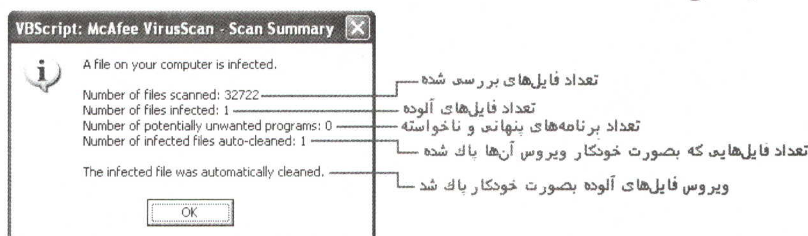
شکل (۵-۱۷) پنجره ویروس‌یابی - انتخاب پوشه‌ها و تنظیمات ویروس‌یابی

☑ *برنامه ویروس‌یاب **McAfee** کلیه فایل‌ها و برنامه‌های را مورد بررسی قرار داده و در صورت یافتن ویروس ، آن را در لیست پایین پنجره نمایش می‌دهد. درصورتیکه ویروس قابل پاک شدن باشد، ویروس را از فایل پاک می‌کند در غیر اینصورت فایل ویروسی را قرنطینه می‌نماید. وضعیت فایل‌های آلوده در قسمت **Status** مشخص شده است.*



شکل (۱۸-۵) پنجره ویروس‌یابی- عملیات ویروس‌یابی

☑ *در پایان پنجره‌ای نمایش داده می‌شود که آماری از فایل‌های بررسی شده و ویروس‌های یافت شده ارائه می‌کند.*



شکل (۱۹-۵) پنجره خلاصه ویروس‌یابی

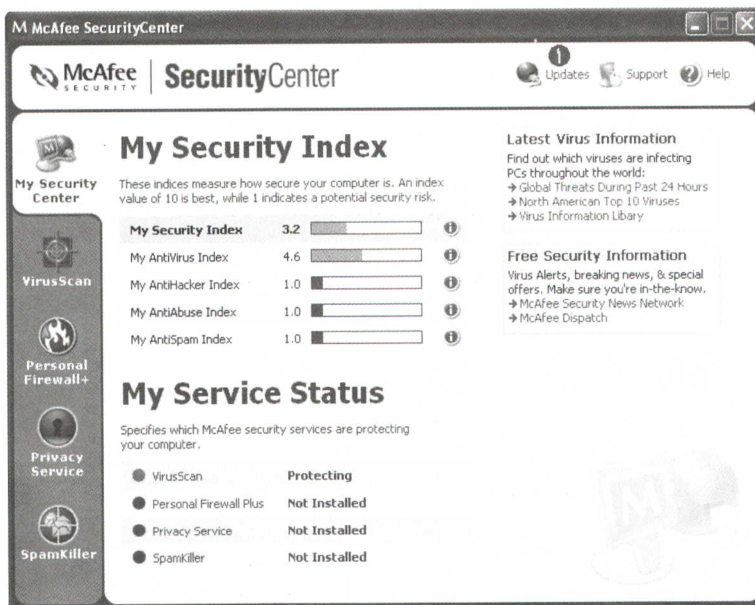
۵-۵ بروزرسانی نرم‌افزار McAfee

همانطور که می‌دانیم ، ممکن است ظرف یک هفته یا چند روز ویروسهای جدیدی توسط افراد خرابکار تولید شود. نرم‌افزارهای ضدویروس فقط قادر به شناسایی ویروسهای شناخته شده هستند بنابراین نیاز است که هر چند روز یکبار آنها را بروزرسانی نماییم. البته نرم‌افزار ضد ویروس **McAfee** از روشی

استفاده می‌کند که ویروسهای جدیدی که ساختاری مشابهی با ویروسهای قدیمی دارند شناسایی می‌کند ولی این نرم‌افزار نیز برای شناسایی ویروسهای با ساختار جدید نیاز به بروزرسانی دارد. شرکتهای تولید کننده نرم‌افزارهای ضد ویروس، آخرین ویروسهای را در سطح دنیا شناسایی می‌کنند و پس از تشخیص عملکرد و نحوه پاک کردن آنها، اطلاعات ویروس و نحوه حذف آن را در سایتهای اینترنتی خود قرار می‌دهند. در ضمن امکان بروزرسانی نرم‌افزارهای ضد ویروس را از طریق اینترنت به کاربران خود می‌دهند.

جهت بروزرسانی نرم‌افزار **McAfee** عملیات زیر را انجام می‌دهیم :

- ☑ *ابتدا به اینترنت متصل می‌شویم.*
- ☑ *بر روی آیکن M در سینی نوار کار، دوبار کلیک می‌کنیم.*
- ☑ *در پنجره اصلی نرم‌افزار **McAfee** بر روی آیکن Updates کلیک می‌کنیم.*



شکل (۲۰-۵) پنجره اصلی نرم‌افزار ضدویروس **McAfee**

- ☑ *در پنجره ظاهر شده توضیح داده شده است که نرم‌افزار **McAfee** بصورت خودکار، عملیات بروزرسانی را انجام می‌دهد (البته اگر به اینترنت متصل باشیم) در این پنجره بر روی دکمه Check Now کلیک می‌کنیم.*



شکل (۲۱-۵) بروزرسانی نرم‌افزار **McAfee**

☑ *نرم‌افزار **McAfee** به سایت وب خود متصل شده و درصورتیکه لازم باشد فایل‌های **Dat** که حاوی اطلاعات شناسایی و پاک کردن ویروسها هستند را بروزرسانی می‌نماید. درصورتیکه نسخه جدیدی از نرم‌افزار **McAfee** نیز وجود داشته باشد با گرفتن اجازه از شما ، نرم‌افزار را دریافت و نصب می‌کند.*



شکل (۲۲-۵) بررسی سایت **McAfee** جهت بروزرسانی نرم‌افزار و فایل‌های **Dat**



۱ - منظور از ضریب امنیتی کامپیوتر در نرم‌افزار McAfee چیست؟ ضریب ۱ و ضریب ۱۰ چه معنایی دارند؟

۲ - برای بالا بردن ضریب امنیتی کامپیوتر چه مواردی را در نرم‌افزار McAfee باید انجام دهیم؟

۳ - دیوار آتش چیست؟ توضیح دهید.

۴ - منظور از قرنطینه کردن فایل‌ها چیست؟

۵ - علت نیاز نرم‌افزارهای ضدویروس به بروزرسانی چیست؟



۱ - سیستم امنیتی را که جهت محافظت از شبکه داخلی در مقابل نفوذ افراد از خارج شبکه طراحی شده است ، را .... می‌گویند.

الف) **Firewall**
ب) **Proxy Server**
ج) **Router**
د) **Security System**

۲ - کدام سربرگ نرم‌افزار **McAfee** وظیفه مقابله با نامه‌های مزاحم و ناخواسته را دارد؟

الف) SpamKiller
ب) Privacy Service
ج) Personal Firewall+
د) VirusScan

۳ - کدام سربرگ نرم‌افزار **McAfee** وظیفه ویروس‌یابی کامپیوتر را دارد؟

الف) My Security Center
ب) SpamKiller
ج) Personal Firewall+
د) VirusScan

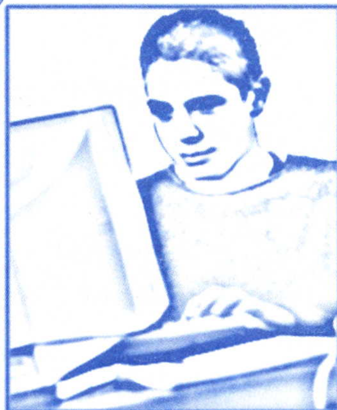
۴ - توسط کدام سربرگ نرم‌افزار **McAfee** می‌توان ضریب وضعیت امنیتی کامپیوتر را مشاهده نمود؟

الف) My Security Center
ب) Personal Firewall+
ج) Privacy Service
د) SpamKiller

۵ - برای بروزرسانی نرم‌افزار **McAfee** از دکمه .... استفاده می‌شود.

الف) **Support**
ب) **Online**
ج) **Update**
د) **Register**

دستور کار آزمایشگاه



۱ - نرم‌افزار **McAfee** را بر روی کامپیوتر خود نصب نمایید.

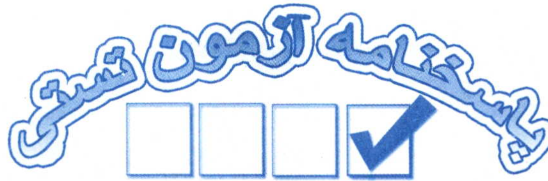
۲ - یک دیسکت را در درایو قرار داده و به کمک نرم‌افزار **McAfee** ویروس‌یابی نمایید.

۳ - یک **CD** را در درایو قرار داده و به کمک نرم‌افزار **McAfee** ویروس‌یابی نمایید. توضیح دهید که اگر بر روی **CD** ویروس قرار داشته باشد چه اتفاقی می‌افتد. آیا می‌توان ویروس را حذف نمود؟

۴ - وضعیت امنیت کامپیوتر خود را بررسی کرده و یادداشت نمایید.

۵ - به کمک نرم‌افزار **McAfee** یک دیسک نجات برای کامپیوتر خود بسازید.

۶ - از طریق اینترنت نرم‌افزار **McAfee** را بروزرسانی نمایید.



فصل	سئوال	الف	ب	ج	د
چهارم	۱	✓			
	۲	✓			
	۳				✓
	۴	✓			
	۵			✓	

توانایی ششم

کار با نرم‌افزار ضدویروس Norton

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☑ نرم‌افزار **Norton Antivirus** را نصب نماید.
- ☑ قسمتهای مختلف نرم‌افزار **Norton Antivirus** را نام برده و کاربرد هر یک را توضیح دهد.
- ☑ عملیات ویروس‌یابی را به کمک نرم‌افزار **Norton Antivirus** انجام دهد.
- ☑ نرم‌افزار **Norton Antivirus** را از طریق اینترنت بروزرسانی نماید.

زمان نظری : -----

زمان عملی : ۴ ساعت

۱-۶ آشنایی با نرم‌افزار Norton Antivirus

این نرم‌افزار توسط شرکت **Symantec** طراحی شده است و در حدود ۲۸٪ بازار نرم‌افزارهای ضدویروس در اختیار این نرم‌افزار است و بیش از ۳۵ میلیون کاربر در سطح دنیا دارد. از مهمترین مزایای این ضدویروس، به روزرسانی ساده و سریع آن توسط سایت **http://www.symantec.com** است. در این کتاب ، از نسخه ۲۰۰۴ نرم‌افزار **Norton Antivirus** استفاده شده است.

۲-۶ نصب نرم‌افزار Norton Antivirus

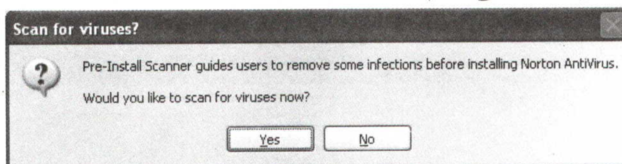
جهت نصب نرم‌افزار **Norton Antivirus** عملیات زیر را انجام می‌دهیم :

☑ *CD نصب نرم‌افزار **Norton Antivirus** را در درایو قرار داده و فایل **NAVSetup.exe** را اجرا می‌کنیم.*



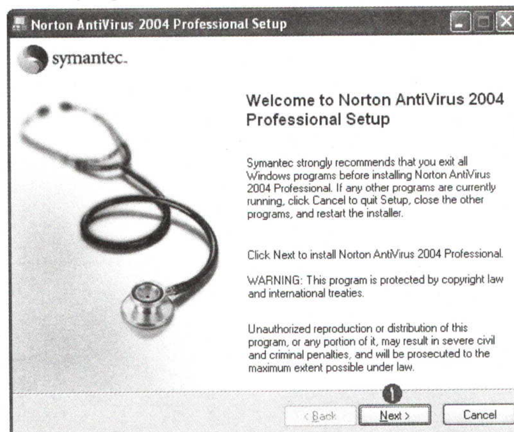
شکل (۱-۶) آیکن برنامه نصب **Norton Antivirus**

☑ *پنجره‌ای مطابق شکل زیر ظاهر می‌شود. در این پنجره سئوال می‌شود که آیا می‌خواهید برنامه نصب ، قبل از نصب ضدویروس **Norton** ، کامپیوتر شما را ویروس‌یابی کند. در صورت تمایل دکمه Yes را کلیک می‌کنیم.*



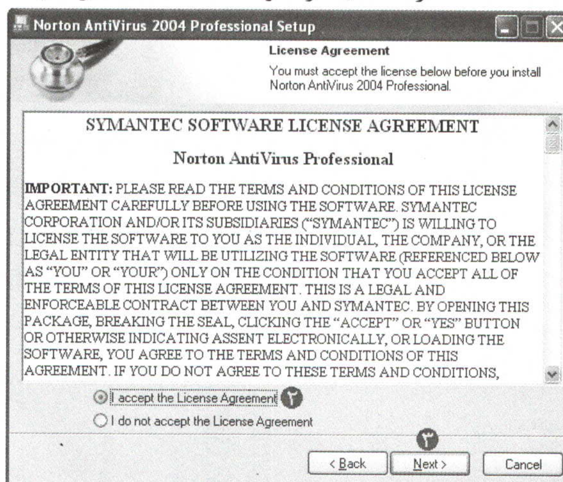
شکل (۲-۶) پنجره محاوره‌ای سئوال در مورد ویروس‌یابی

☑ *پنجره خوش‌آمد گویی نصب ظاهر می‌شود. دکمه Next > را جهت ادامه نصب کلیک می‌کنیم.*



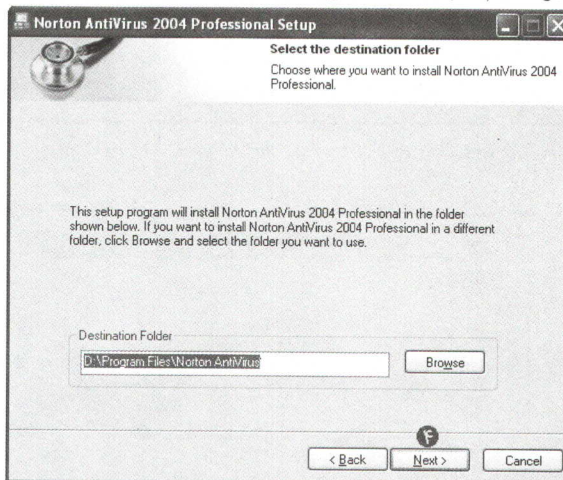
شکل (۳-۶) پنجره خوش‌آمدگویی نصب **Norton Antivirus 2004**

☑ در پنجره بعد، موافقتنامه مجوز استفاده از نرم‌افزار نمایش داده می‌شود. برای قبول این موافقتنامه، گزینه I accept the License Agreement را انتخاب کرده و دکمه Next > را کلیک کنید.



شکل (۴-۶) پنجره موافقتنامه مجوز استفاده از نرم‌افزار **Norton Antivirus 2004**

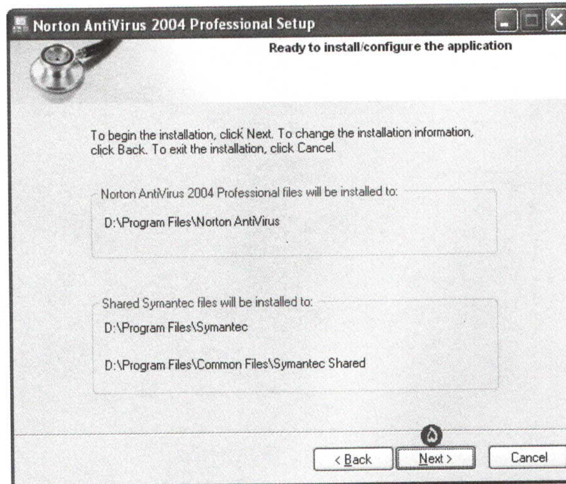
☑ در پنجره بعدی محل نصب نرم‌افزار مشخص شده است. می‌توانیم به کمک دکمه Browse... محل نصب برنامه را تغییر دهیم. جهت ادامه کار دکمه Next > را کلیک می‌کنیم.



شکل (۵-۶) پنجره تعیین محل نصب نرم‌افزار

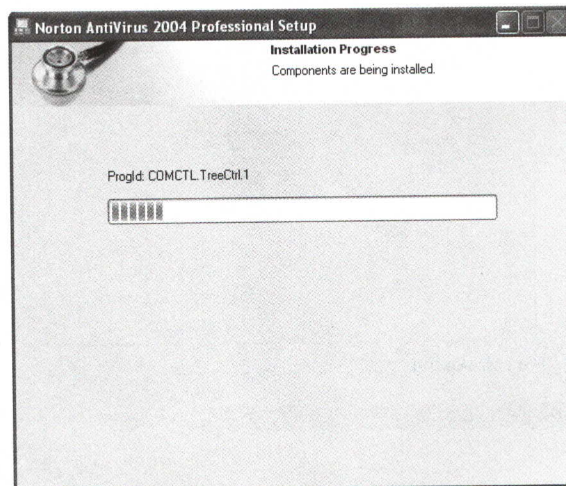
☑ در پنجره بعد، محل نصب نرم‌افزار و محل کپی کردن فایل‌های مورد نیاز آن نمایش داده می‌شود. اگر می‌خواهید این محل‌ها را تغییر دهید، دکمه < Back را کلیک کنید. برای ادامه نصب دکمه Next > را کلیک نمایید.





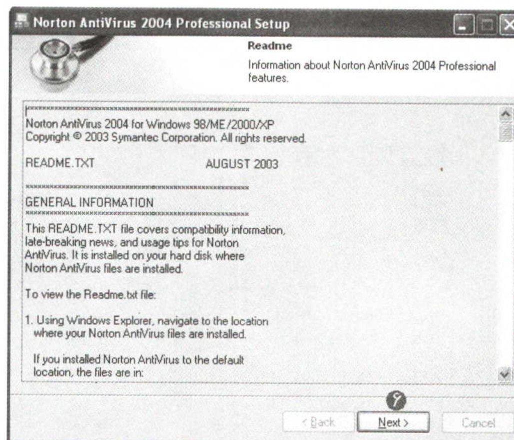
شکل (۶-۶) پنجره نمایش محل نصب نرم‌افزار

☑ پنجره کپی کردن فایل‌های نرم‌افزار **Norton Antivirus** ظاهر می‌شود و عملیات کپی فایل‌ها انجام می‌شود.



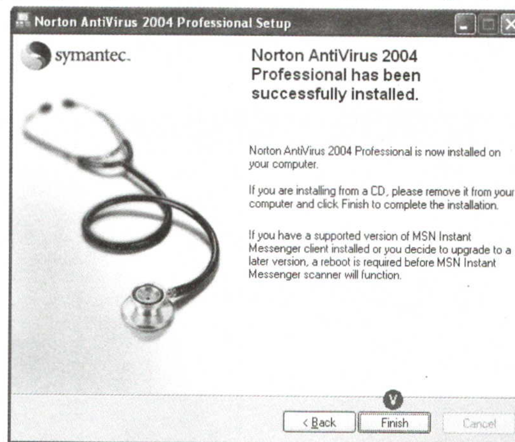
شکل (۷-۶) پنجره کپی فایل‌ها و عملیات نصب نرم‌افزار **Norton Antivirus**

☑ بعد از انجام عملیات نصب، پنجره **Readme** ظاهر می‌شود. در این پنجره توضیحاتی در مورد امکانات و نحوه استفاده از نرم‌افزار **Norton Antivirus** نمایش داده شده است. برای ادامه کار دکمه Next > را کلیک می‌کنیم.



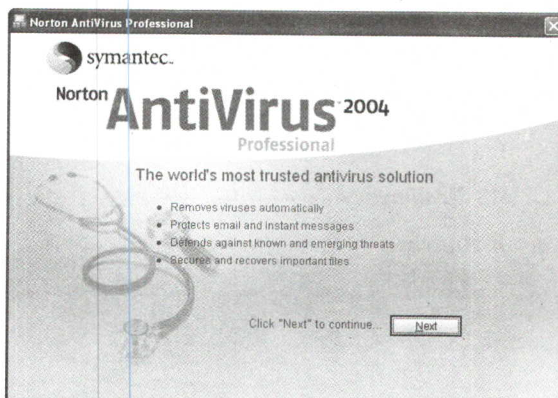
شکل (۸-۶) پنجره **Readme**

☑ پنجره پایانی نصب ظاهر می‌شود. بر روی دکمه Finish کلیک می‌کنیم.



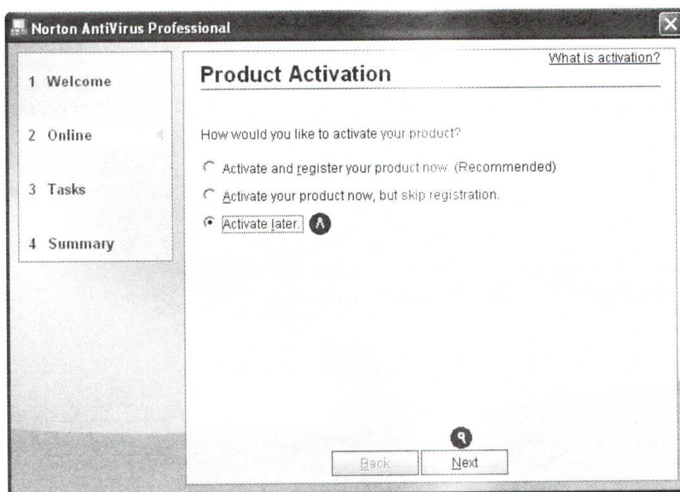
شکل (۹-۶) پنجره پایانی نصب نرم‌افزار **Norton Antivirus**

☑ پس از اتمام عملیات نصب ، پنجره‌ای مطابق شکل زیر ظاهر می‌شود. در این پنجره دکمه Next > را کلیک می‌کنیم.



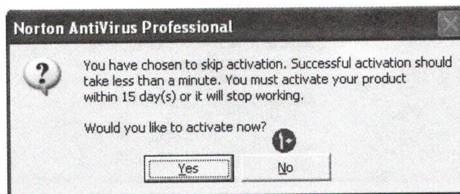
شکل (۱۰-۶) پنجره معرفی نرم‌افزار **Norton Antivirus**

☑ در پنجره بعد از ما خواسته می‌شود که نرم‌افزار خود را فعال کنیم. در صورتیکه نرم‌افزار نصب شده کپی غیر مجاز نباشد و به اینترنت نیز متصل باشیم ، گزینه اول را انتخاب کرده و دکمه Next را کلیک می‌کنیم تا نرم‌افزار **Norton Antivirus** خود را فعال کنیم. در غیر اینصورت گزینه سوم (Activate later فعال سازی در آینده) را انتخاب کرده و دکمه Next را کلیک می‌کنیم.



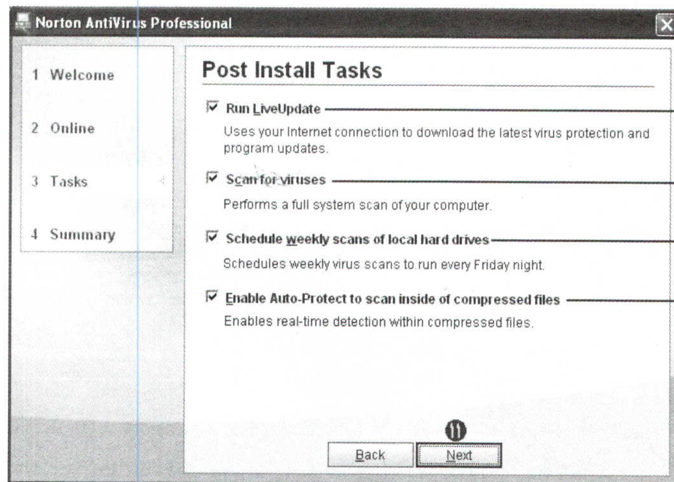
شکل (۱۱-۶) پنجره فعال سازی نرم‌افزار **Norton Antivirus**

☑ در صورتیکه در پنجره قبل گزینه سوم را انتخاب کرده باشیم ، پنجره‌ای ظاهر می‌شود با این پیغام که شما باید نرم‌افزار خود را ظرف مدت ۱۵ روز فعال نمایید. آیا می‌خواهید حالا نرم‌افزار خود را فعال کنید؟ دکمه No را کلیک می‌کنیم.



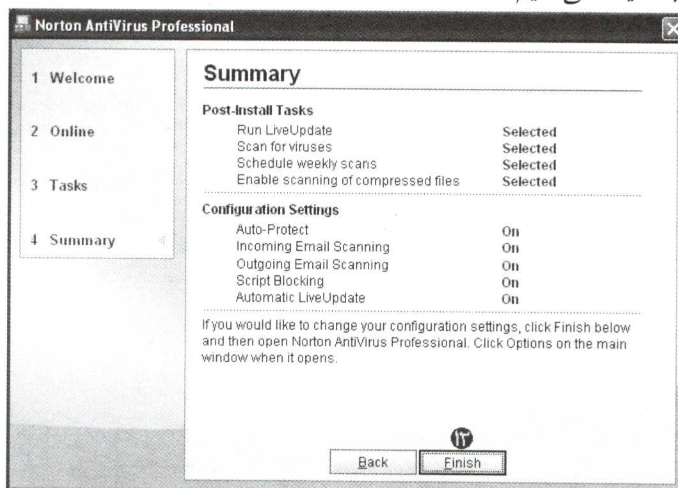
شکل (۱۲-۶) پنجره سئوال در مورد فعال سازی

☑ در پنجره بعدی کارهایی که نرم‌افزار **Norton Antivirus** باید انجام دهد مشخص می‌شود. موارد مورد نظر را انتخاب کرده و دکمه Next را کلیک می‌کنیم.



شکل (۱۳-۶) پنجره تعیین کارهایی که نرم‌افزار **Norton Antivirus** باید انجام دهد

☑ در پایان خلاصه‌ای از کارهای انجام شده نمایش داده می‌شود. دکمه Finish را جهت اتمام عملیات نصب کلیک می‌کنیم.



شکل (۱۴-۶) خلاصه‌ای از عملیات و تنظیمات انجام شده

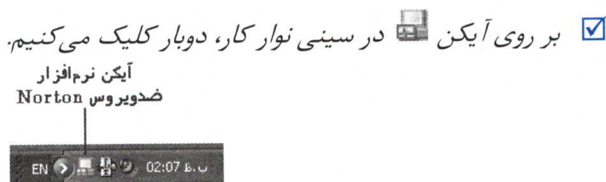
۶-۳ شناسایی و پاکسازی ویروسها با نرم‌افزار Norton Antivirus

همانند نرم‌افزار **McAfee** نرم‌افزار **Norton Antivirus** نیز پس از نصب، بصورت مقیم در حافظه قرار می‌گیرد. در ضمن هربار که کامپیوتر را روشن کنیم این نرم‌افزار به صورت خودکار اجرا شده و در حافظه قرار می‌گیرد. هر فایل یا پوشه‌ای را که باز کنیم، نرم‌افزار **Norton** بصورت خودکار فایل‌های داخل آن را پوشه را بررسی می‌کند و درصورتیکه فایل ویروسی پیدا کند بلافاصله پیغامی را نمایش می‌دهد و از فعالیت ویروس جلوگیری می‌کند.

گاهی اوقات ممکن است بخواهیم تمام یا بخشی از فایل‌های کامپیوتر را ویروس‌یابی کنیم.

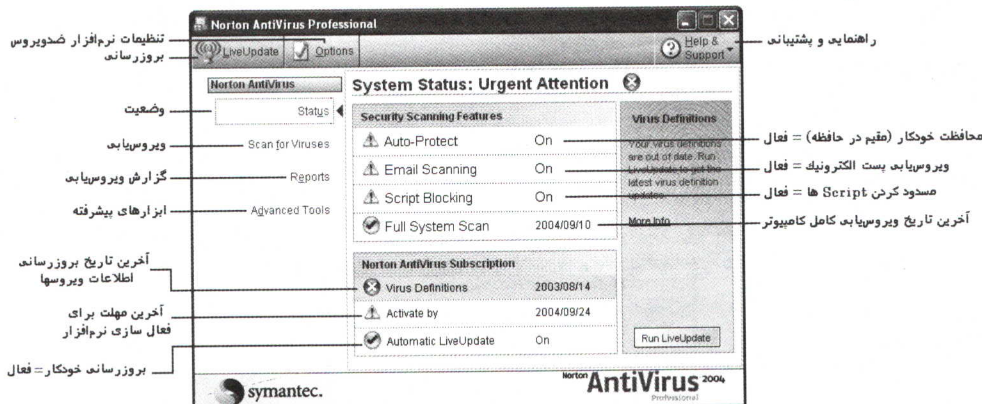
برای ویروس‌یابی کامپیوتر عملیات زیر را انجام می‌دهیم :

☑ *بر روی آیکن در سینی نوار کار، دوبار کلیک می‌کنیم.*



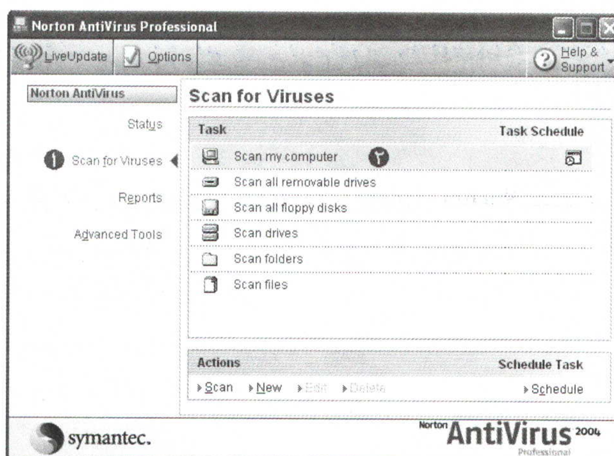
شکل (۱۵-۶) آیکن نرم‌افزار ضدویروس **Norton**

☑ *پنجره برنامه ضدویروس **Norton** ظاهر می‌شود. در این پنجره مشخصاتی از وضعیت فعلی و عملیات گذشته ضدویروس نمایش داده می‌شود. جهت ویروس‌یابی بر روی دکمه* Scan for Viruses *کلیک می‌کنیم.*



شکل (۱۶-۶) پنجره اصلی نرم‌افزار **Norton Antivirus** – قسمت **Status**

☑ *پنجره‌ای مطابق شکل زیر ظاهر می‌شود.*



شکل (۱۷-۶) نرم‌افزار **Norton Antivirus** قسمت **Scan for Viruses**

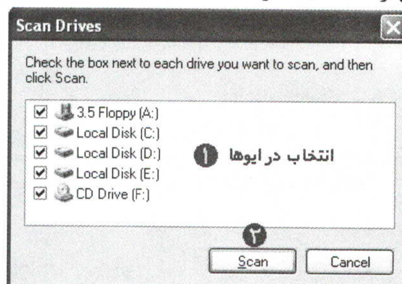
در این پنجره دکمه‌های زیر وجود دارد :

- Scan my computer
با دوبار کلیک بر روی این دکمه، کلیه فایل‌های موجود در کامپیوتر ویروس‌یابی می‌شود.

- Scan all removable drives
با دوبار کلیک بر روی این دکمه ، کلیه درایوهای قابل جابجایی نظیر فلاپی دیسک، **CD Drive** ، **Flash Disk** و ... ویروس‌یابی می‌شود.

- Scan all floppy disks
با دوبار کلیک بر روی این دکمه ، تمامی درایوهای فلاپی موجود در کامپیوتر ویروس‌یابی می‌شود.

- Scan drives
با دوبار کلیک بر روی این دکمه ، پنجره‌ای باز می‌شود که می‌توان درایو یا درایوهای مورد نظر جهت ویروس‌یابی را انتخاب نمود.



شکل (۱۸-۶) پنجره انتخاب درایوها جهت ویروس‌یابی

- Scan folders

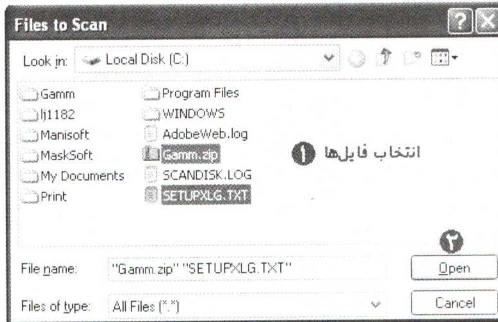
با دوبار کلیک بر روی این دکمه ، پنجره‌ای باز می‌شود که می‌توان پوشه یا پوشه‌های مورد نظر جهت ویروس‌یابی را انتخاب نمود.



شکل (۱۹-۶) پنجره انتخاب پوشه‌ها جهت ویروس‌یابی

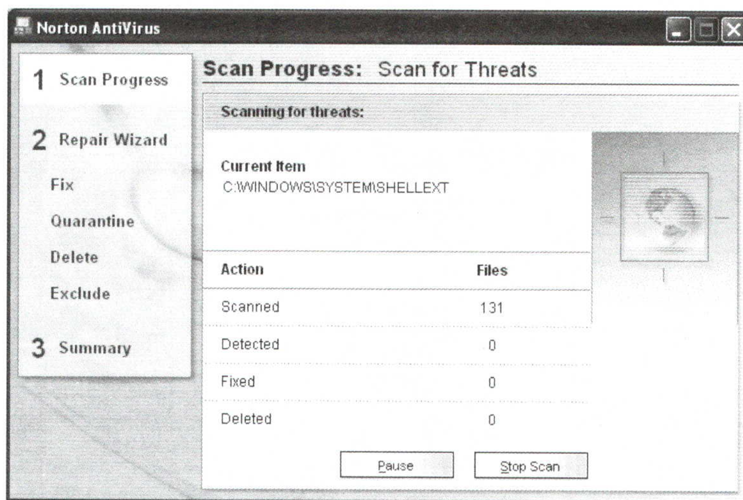
- Scan files

با دوبار کلیک بر روی این دکمه ، پنجره‌ای باز می‌شود که می‌توان فایل یا فایل‌های مورد نظر جهت ویروس‌یابی را انتخاب نمود.



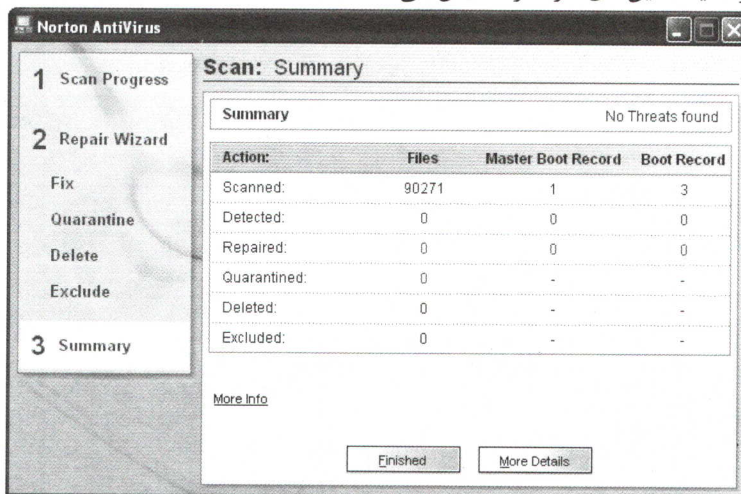
شکل (۲۰-۶) پنجره انتخاب فایل‌ها جهت ویروس‌یابی

☑ *پس از انجام یکی از موارد فوق ، پنجره‌ای مطابق شکل زیر باز می‌شود و فایل‌ها ، پوشه‌ها یا درایوهایی که مشخص کرده‌ایم را ویروس‌یابی می‌کند.*



شکل (۲۱-۶) پنجره ویروس‌یابی فایل‌ها و پوشه‌های تعیین شده

☑ درصورتیکه فایل ویروسی در کامپیوتر پیدا شود، نرم‌افزار ***Antivirus*** ویروس فایل آلوده را پاک می‌کند. در پایان گزارشی نمایش داده می‌شود که تعداد فایل‌های بررسی شده و تعداد فایل‌های آلوده و وضعیت فایل‌های آلوده را نمایش می‌دهد.



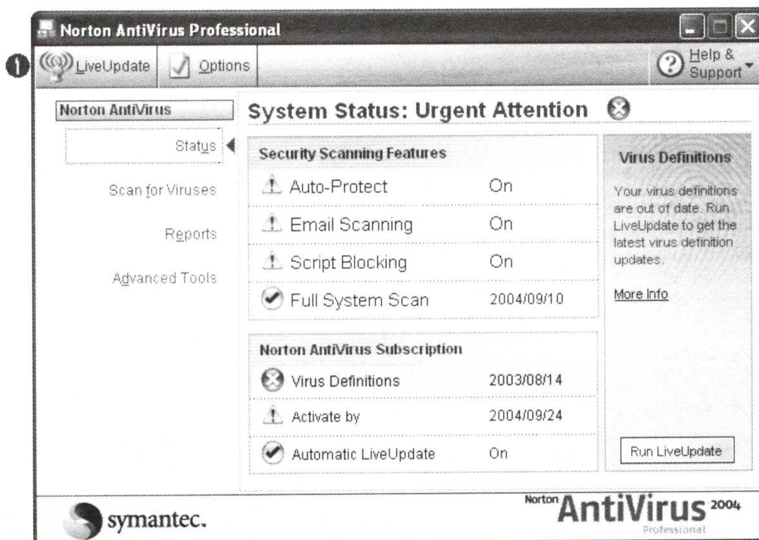
شکل (۲۲-۶) پنجره نمایش نتیجه عملیات ویروس‌یابی

۶-۴ بروزرسانی نرم‌افزار Norton Antivirus

همانطور که در فصل قبل نیز اشاره کردیم ، ممکن است ظرف یک هفته یا چند روز ویروسهای جدیدی توسط افراد خرابکار تولید شود. نرم‌افزارهای ضدویروس فقط قادر به شناسایی ویروسهای شناخته شده هستند بنابراین نیاز است که هر چند روز یکبار آنها را بروزرسانی نماییم. شرکتهای تولید کننده نرم‌افزارهای ضد ویروس، آخرین ویروسهای را در سطح دنیا شناسایی می‌کنند و پس از تشخیص عملکرد و نحوه پاک کردن آنها، اطلاعات ویروس و نحوه حذف آن را در سایتهای اینترنتی خود قرار می‌دهند. در ضمن امکان بروزرسانی نرم‌افزارهای ضد ویروس را از طریق اینترنت به کاربران خود می‌دهند.

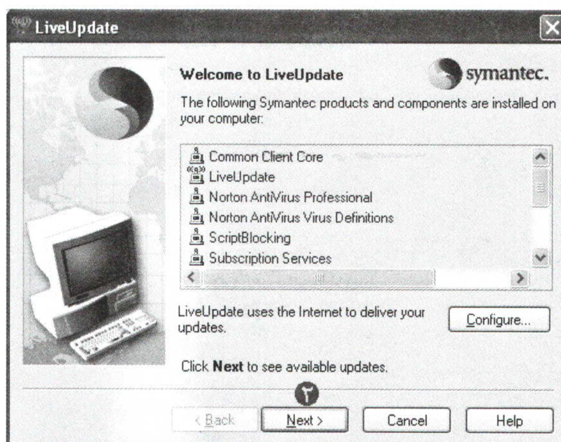
جهت بروزرسانی نرم‌افزار Norton Antivirus عملیات زیر را انجام می‌دهیم :

- ☑ *ابتدا به اینترنت متصل می‌شویم.*
- ☑ *بر روی آیکن در سینی نوار کار، دوبار کلیک می‌کنیم.*
- ☑ *در پنجره اصلی نرم‌افزار **Norton Antivirus** بر روی دکمه LiveUpdate کلیک می‌کنیم.*



شکل (۶-۲۳) پنجره اصلی برنامه Norton Antivirus

- ☑ *پنجره **Live Update** ظاهر می‌شود. در این پنجره دکمه Next > را کلیک می‌کنیم.*



شکل (۲۴-۶) پنجره **Live Update**

☑ *برنامه **Live Update** به اینترنت متصل شده و اطلاعات شناسایی و حذف ویروسهای جدید را دریافت می‌کند.*



۱ - وظیفه برنامه Live Update در نرم‌افزار Norton Antivirus چیست؟

۲ - علت بروزرسانی نرم‌افزارهای ضدویروس چیست؟



۱ - کدام نرم‌افزار ضد ویروس زیر توسط شرکت **Symantec** طراحی شده است؟

الف) **Dr Web** ب) **Norton Antivirus**

ج) **McAfee Virus Scan** د) **Panda Antivirus**

۲ - کدام نرم‌افزار زیر ضدویروس محسوب نمی‌شود؟

الف) **Norton Utility** ب) **Norton Antivirus**

ج) **McAfee** د) **Panda**

۳ - برای بروزرسانی نرم‌افزار **Norton Antivirus** از کدام دکمه استفاده می‌شود؟

الف) **Status** ب) **Online** ج) **Live Update** د) **Register**

۴ - در نرم‌افزار **Norton Antivirus** برای ویروس‌یابی یک فایل در درایو **C** بهتر است از کدام دکمه زیر استفاده شود؟

الف) Scan my computer ب) Scan folders ج) Scan drives د) Scan files

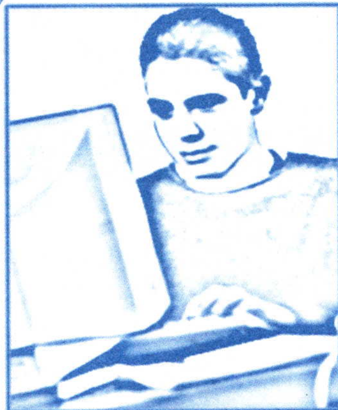
۵ - در نرم‌افزار **Norton Antivirus** برای ویروس‌یابی فلاپی دیسک بهتر است از کدام دکمه زیر استفاده شود؟

الف) Scan my computer ب) Scan all floppy disks

ج) Scan folders د) Scan files



دستور کار آزمایشگاه



۱ - نرم‌افزار **Norton Antivirus** را بر روی کامپیوتر خود نصب نمایید.

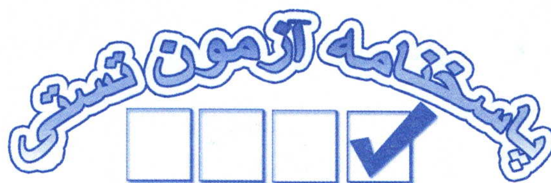
۲ - یک دیسکت را **Write Protect** کرده و در درایو قرار داده و به کمک نرم‌افزار **Norton Antivirus** ویروس‌یابی نمایید. در صورت یافتن ویروس چه اتفاقی می‌افتد؟

۳ - درایو **C** کامپیوتر را ویروس‌یابی نمایید.

۴ - فقط پوشه ویندوز را ویروس‌یابی نمایید.

۵ - فقط فایل **Calc.exe** در پوشه **Windows\system32** را ویروس‌یابی نمایید.

۶ - از طریق اینترنت نرم‌افزار **Norton Antivirus** را بروزرسانی نمایید.



فصل	سئوال	الف	ب	ج	د
ششم	۱		✓		
	۲	✓			
	۳			✓	
	۴				✓
	۵		✓		